Exhibit 2

CLAIM NO. KB-2023-002877

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION

BETWEEN

(1) NICHOLAS DEL ROSSO
(2) VITAL MANAGEMENT SERVICES INC

Claimants

-and-

STOKOE PARTNERSHIP SOLICITORS

Defendant

EXPERT REPORT OF PHIL BECKETT

9 February 2024

ALVAREZ & MARSAL DISPUTES & INVESTIGATIONS LLP

Contents

Redacted

ATTACHMENTS TO THE REPORT

APPENDICES

Appendix	Description
PB1-01	Curriculum vitae of Phil Beckett
PB1-02	The Order
PB1-03	Diligence Report
PB1-04	Instructions
PB1-05	Security Overview

1 Introduction

1.1 Expert

1.1.1 I am a Managing Director at Alvarez & Marsal ("A&M") and lead their Disputes & Investigations practice in Europe and the Middle East. I, specifically work within the Forensic Technology team, where I have more than 20 years' experience providing expert opinion and evidence on related technology issues, including computer forensics, eDisclosure, data analytics and software development.

1.1.2 I joined A&M after spending two years as a Partner at Proven Legal Technologies Limited, a full-service e-Discovery and Forensic Computing company based in London. Prior to this I spent seven years leading the European Forensic Technology practice at Navigant Consulting Inc. I have held similar roles at BDO Stoy Hayward and Andersen.

1.1.3 I have a Master's in Forensic Computing from Cranfield University, a Master's in Computer and Communications Law from Queen Mary University of London and am a Fellow of the Association of Chartered Certified Accountants ("ACCA"), having won the ACCA Gold Medal in 2001.

1.1.4 I specialise in advising clients in relation to the preservation and investigation of digital evidence, the interrogation of complex data sets and the disclosure of electronic documents. I am a Certified Fraud Examiner and have been a recognised court expert in relation to various aspects of digital evidence, producing numerous expert reports.

1.1.5 I have extensive experience in the forensic technology field and have been involved in numerous projects, within which I have been responsible for the collection, processing and review of electronic data to meet a range of legal requirements from various jurisdictions, including the US, Canada, Hong Kong, Dubai, the EU and the UK.

1.1.6 A copy of my curriculum vitae is attached at **Appendix PB1-01**.

1.2 Instructions

1.2.1 I am instructed on this matter by Rosenblatt (**"Rosenblatt"** or "**Instructing Solicitors**"), acting on behalf of Nicholas del Rosso (the **"Defendant"**), in a High Court claim (the **"Claim"**) against Stokoe Partnership Solicitors (the **"Claimant"**).

1.2.2 My instructions in part relate to a court order issued by The Honourable Mr justice Michael Green on 9 October 2023 (the "**Order**") and a forensic report issued by Diligence International Limited ("**Diligence**") on 12 January 2023 (the "**Diligence Report**"). A copy of the **Order** is attached to this Report as **Appendix PB1-02** and a copy of the **Diligence Report** is attached to this Report as **Appendix PB1-03**.

1.2.3 My instructions ("**Instructions**") are attached to this Report as **Appendix PB1-04**.

1.2.4 Specifically, I have been instructed to consider, investigate, and opine on issues, as defined strictly in and only in my Instructions. In summary, these issues are:

i) Upon collection of the Laptop and the associated/Dedicated Media

a) Record the condition upon which A&M took receipt of all items.

b) Review all items provided so as to verify that they accord with the signed Summary of Media provided by the Claimant on 11 August 2023.

c) Review all items so as to be able to carry out the requirements of the investigations pursuant to the Order as follows.

ii) Determine (insofar as is possible) and produce a report ("the Independent Forensic Report") addressing the following matters:

a) Whether a backup file of an email account relating to Scott Michael Moore of Moore International PLLC ("the Moore Data") is on the Laptop, as alleged by Diligence in its report of 12 January 2023;

b) If so, the date on, and full particulars of how, the Moore Data came to be on the Laptop; and

c) Details of any access to the Laptop which has taken place since 24 October 2020, including details of when and where that access took place, by whom and what activity and/or operations were performed on the Laptop.

iii) If the Moore Data is present on the Laptop and/or Dedicated Media:

a) Remove the Moore Data from the Laptop and Dedicated Media.

b) Create a forensic image of the Laptop's hard drive ("the Amended Laptop Image").

c) Provide the Moore Data to Moore International Law PLLC by a means to be agreed between Rosenblatt and Moore International Law PLLC.

iv) If the Moore Data is not present on the Laptop, create a forensic image of the Laptop's hard drive ("the Laptop Image").

v) Use all reasonable endeavours to search the Laptop for the passcode/password for the Aegis device ("Aegis Device") (including any such password contained within any password manager on the Laptop).

vi) In performing the above tasks, take steps to minimise the possibility of data on the Laptop or master copies being altered.

vii) Prepare a report that sets out my findings and address the issue as to whether or not the date settings on the Laptop are approximately one year out.

viii) Provide the Aegis Drive password, if located, and set out the search terms utilised when looking for the password.

1.3 Background of the dispute

1.3.1 Rosenblatt provided facts in regard to the background of the dispute, which have been provided below, insofar as is necessary for a proper understanding of this report.

i) The Defendant purchased the Laptop in March 2019 on Amazon which was delivered to his address in North Carolina, United States.

ii) In 2019 the Laptop was brought to London, United Kingdom by the Defendant and used while the Defendant was giving evidence in the RAKIA v Azima trial.

iii) On 1 February 2020 the Laptop was left in London by the Defendant at his rented property and he returned to the United States.

iv) On 24 October 2020 the Defendants son, Leo Del Rosso ("Leo") meets Mr McIntyre to provide him (Mr McIntyre) the laptop.

v) On 14 July 2022 Mr McIntyre attends the London office of the Claimant and delivers the Laptop, which the Claimant accepts. The Claimant gives the Laptop to Diligence.

vi) On 28 October 2022 the Claimant instructs Diligence to, amongst other things, try to identify who the Laptop belongs to.

vii) On 3 November 2022 Diligence access the Laptop.

viii) On 12 January 2023 Diligence provide the Claimant with the Diligence Report setting out their findings from their analysis of the Laptop.

ix) On 11 August 2023 the Claimant delivered the Laptop and Dedicated Media to Rosenblatt.

1.4 Other matters

1.4.1 This Report has been prepared from information provided to me by my Instructing Solicitors. The electronic data sources provided to me were preserved in a forensically sound manner prior to being analysed for the purposes of opining on the issues stated in my Instructions.

1.4.2 A list and explanation of these data sources can be found at Section 5 of this report.

1.4.3 All data sources provided to me in this matter are assumed to be true, accurate and in use at the appropriate time. I take no responsibility for the completeness of data, or other information provided to me as part of this engagement.

1.4.4 The opinions I have expressed in this Report are necessarily based on the information provided to me. Should further information become available after the date of this Report which, on consideration by me, affects the findings or opinions stated in this Report, then I will issue an amendment to this Report to modify my opinions where necessary. I acknowledge that I have a duty to do so.

1.4.5 This Report must not be construed as expressing opinions on matters of law, which are for the High Court to determine, although it necessarily reflects my understanding of certain legal matters. This Report has been prepared solely for use in these proceedings between the parties to this matter and their advisers. This Report should not be used, reproduced or circulated for any other purpose or without my prior written consent. My firm accepts no responsibility to third parties for any breaches of this obligation.

1.4.6 I have been assisted in the preparation of this Report by members of my team working under my supervision. All opinions expressed in this Report are my own. I, and my firm, do not have nor have we had any interest in the parties to this litigation nor any personal interests in this matter. My firm's compensation is not contingent upon any actions or events resulting from opinions or conclusions in this Report.

1.5 Structure of this Report

1.5.1 This Report comprises the following sections:

i) **Introduction** (this Section)

ii) **Summary of Conclusions** sets out a summary of my conclusions for the issues defined in the Instructions.

iii) **Chain of Custody** sets out the chain of custody for the Laptop and Dedicated Media since being in A&M's possession.

iv) **Security** sets out the A&M's security and safeguards of the Laptop and Dedicated Media while in A&M's possession.

v) **Electronic Data Sources** sets out the data sources used by me for the purposes of opining on the issues stated in the Instructions.

vi) **Key Concepts** sets out key concepts related to forensic artefacts and metadata examined in this report.

vii) **My Methodology** sets out my methodology in relation to my analysis.

viii) **Analysis** sets out the results of my analysis.

ix) **Conclusion** sets out my conclusion and responses to the issues defined in the instructions.

x) **Caveat to Conclusions**

xi) **Expert Declaration** sets out my signed Expert Declaration.

2 Summary of conclusions

2.1.1 I have been instructed on this matter by **Rosenblatt** to provide an opinion on certain technical aspects of the matter as set out in Section 1.2 of my report. I have been assisted in the preparation of this report by members of my team working under my supervision.

2.1.2 I have reviewed a number of sources as part of my analysis, including the Order of The Honourable Mr Justice Michael Green made on 9 October 2023 and a forensic report issued by Diligence International Limited on 12 January 2023. I have also analysed the electronic sources as set out in Section 5 of my report.

3 Chain of Custody

3.1 Collection and Review of Laptop and Dedicated Media

3.1.1 On 19 October 2023 my colleague, Christian Hill, attended the London office of Rosenblatt, 165 Fleet St, London EC4A 2DY, and took receipt of the Laptop and Dedicated Media.

3.1.2 Upon Mr Hill's return to A&M's London Office, Park House 16-18 Finsbury Circus, London EC2M 7EB, the Laptop and Dedicated Media were taken to the secure forensic laboratory within A&M's London Office.

3.1.3 The Laptop and Dedicated media were removed from the sealed evidence bag G125588 and catalogued and tracked in A&M's evidence tracking system. Within evidence bag G125588, the exhibits were also contained in individual evidence bags (see Section 5) which they were removed from for cataloging.

3.1.4 On 19 October 2023, upon completion of cataloguing and tracking, the Laptop and Dedicated media were sealed in the evidence bag L00488887 and stored in A&M's secure evidence room. Exhibit COUAE008 was sealed separately in the evidence bag S01554796 per the Claimants request for it to be returned.

3.2 Imaging and Verification

3.2.1 On 23 October 2023 the Laptop and Dedicated Media in sealed evidence bag L00488887 were removed from A&M's secure evidence room for imaging and verification in A&M's secure forensic laboratory. The details of the imaging and verification have been provided in Section 5 of this report.

3.2.2 On 27 October 2023 upon completion of imaging and verification, the Laptop and Dedicated were returned to A&M's secure evidence room in sealed evidence bag L00482792.

4 Security

4.1 A&M Security Overview

4.1.1 At Alvarez & Marsal (A&M), we understand our role as trusted stewards for our clients' most important and valuable assets: their data. A&M's Cybersecurity Program employs a layered, defense-in-depth strategy to protect information assets and systems. Core pillars of this Program include Data Governance, Boundary Defense, Access Control, Endpoint Security, Threat Prevention/Monitoring, Vulnerability Management, Business Continuity, Physical Security, and enterprise-wide Security Awareness. These safeguards, along with a dedicated security function have been implemented to ensure the confidentiality, integrity, and availability of A&M and client data.

4.1.2 A&M maintain ISO/IEC 27001:2013 certification for our datacentres and forensic labs in the UK and Germany under Certification Number 12 310 56289 TMS., issued by The Certification Body of TÜV SÜD Management Service GmbH on 13/08/2018 and is renewed annually. Additionally, in line with the firm's commitment to cybersecurity, A&M is Cyber Essentials PLUS certified, which consists of an annual independent third-party assessment of A&M's security practices. For verification of certification and additional information, please see https://www.cyberessentials.ncsc.gov.uk/.

4.1.3 For the A&M's full security overview, please see Appendix PB1-05

4.2 Matter Specific Security

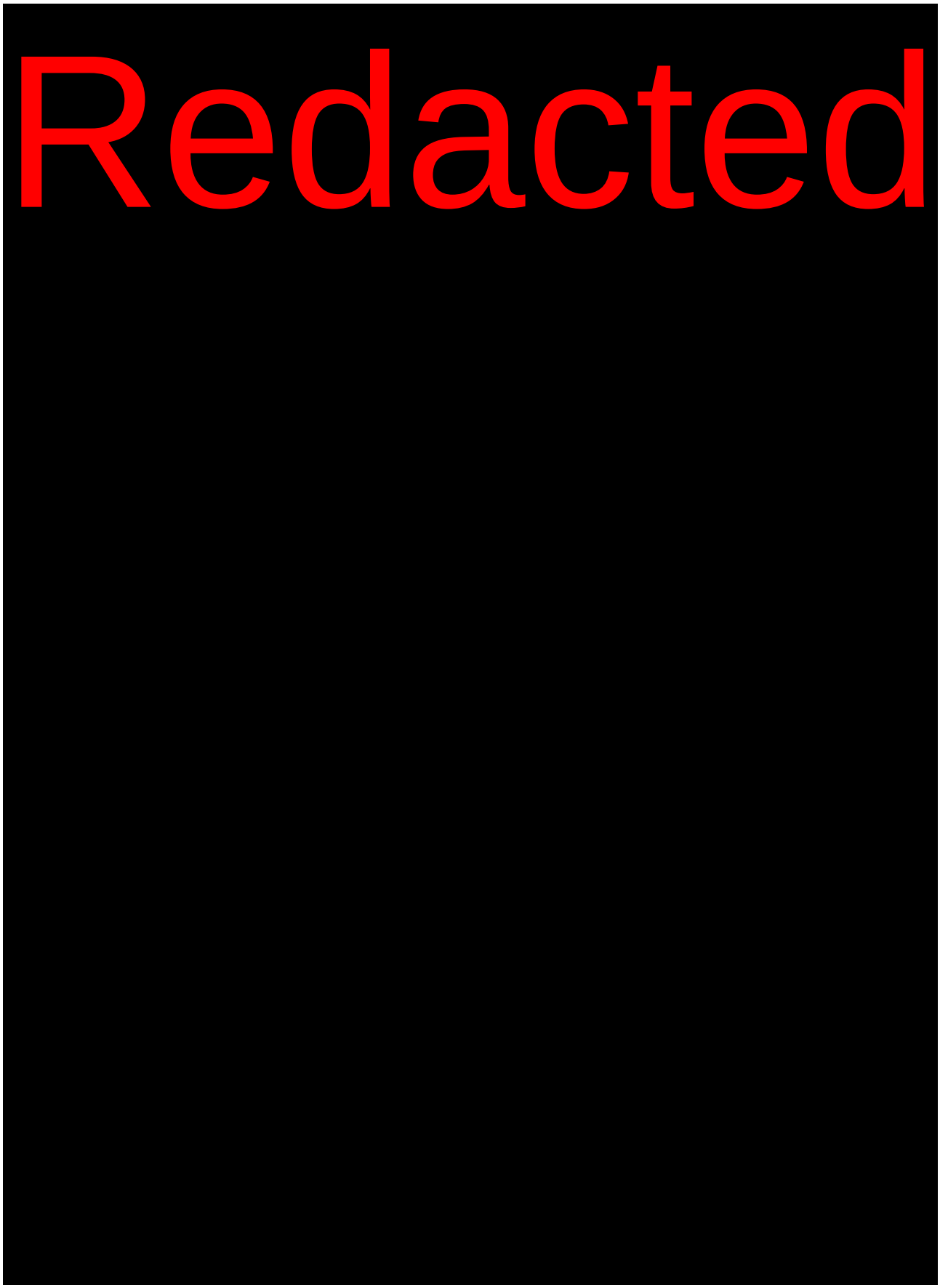
4.2.1 On 31 August 2023 I submitted a letter to Rosenblatt in regard to the security of information held by A&M on this matter in respect of a prior instruction. Please see Appendix PB1-06.

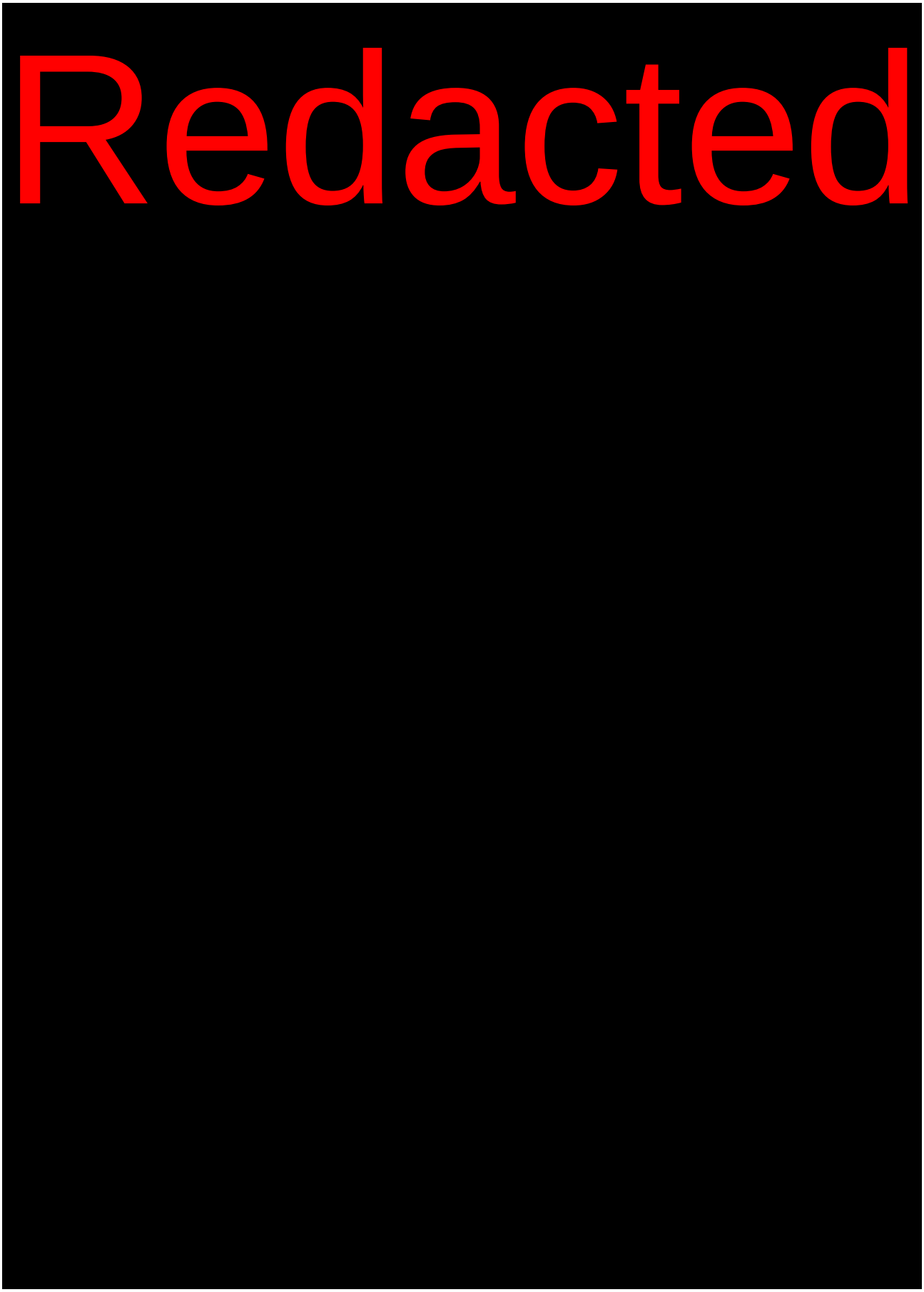
4.2.2 A&M's Disputes & Investigation practice infrastructure team created a data barrier by providing a secure designated area on the forensic network to which only the project team has access.

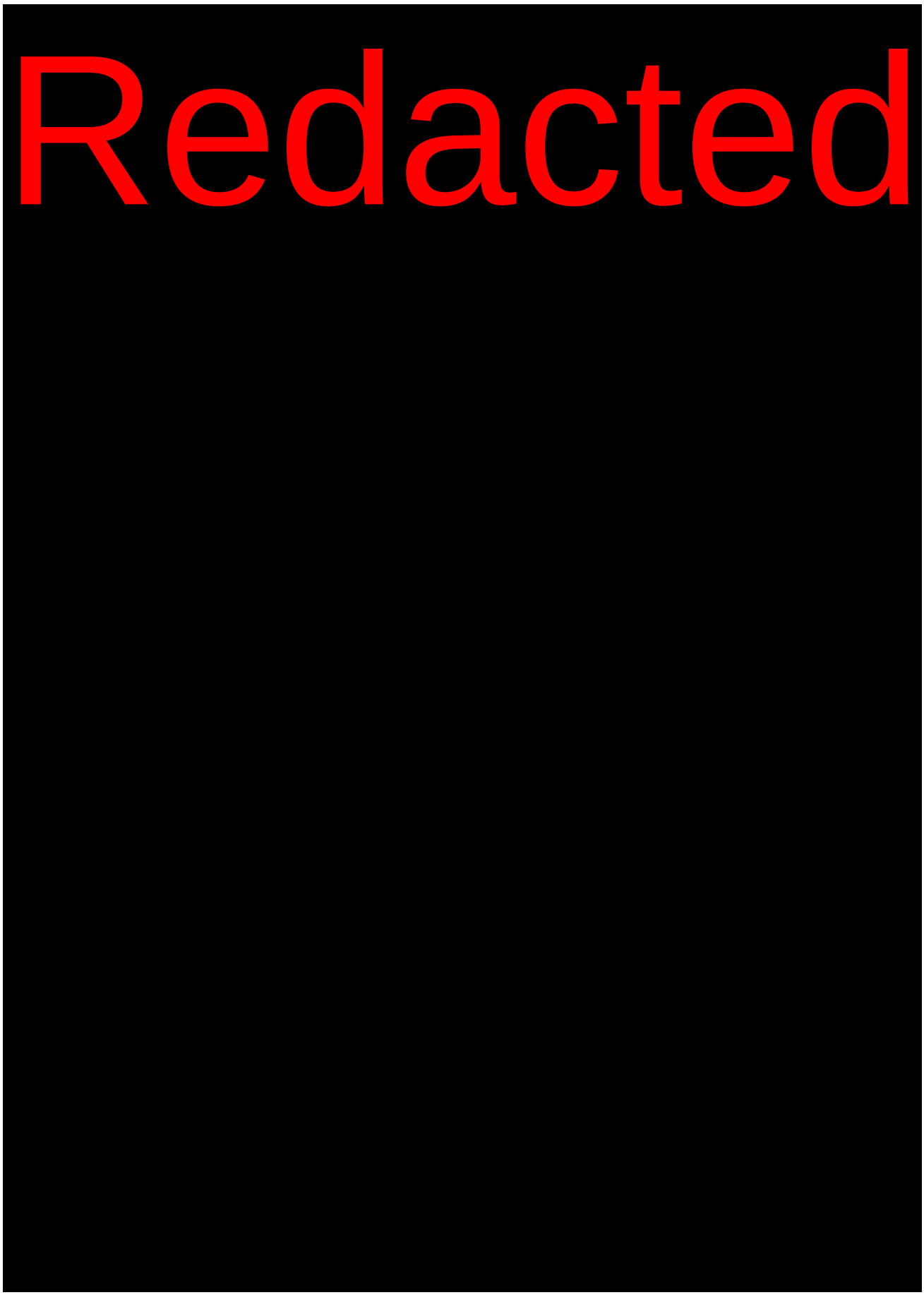
4.2.3 All physical items have been stored in evidence bags within A&M's secure evidence room while not being examined.

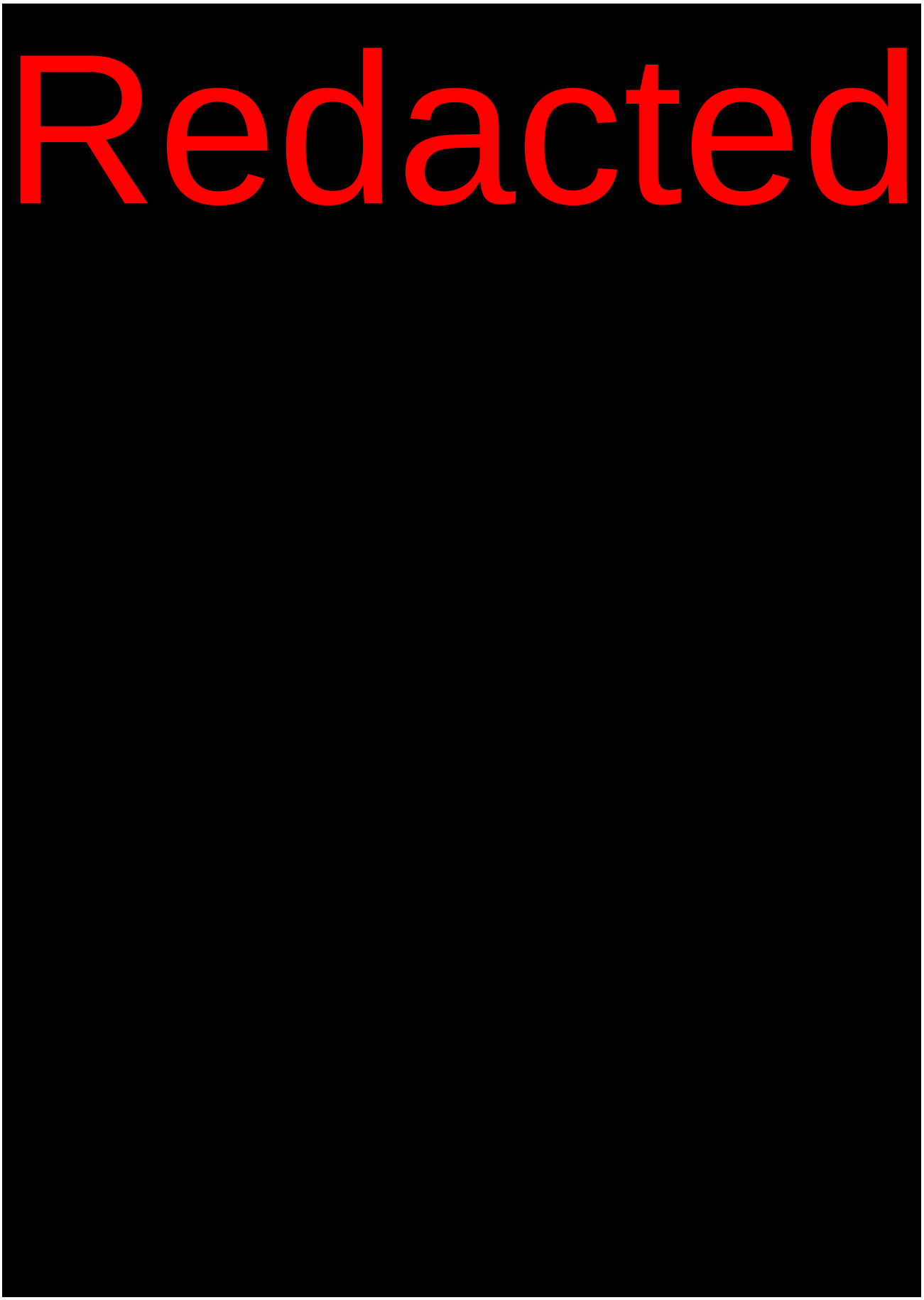
4.2.4 All digital evidence and derived files have been stored in the secure designated area on the forensic network.

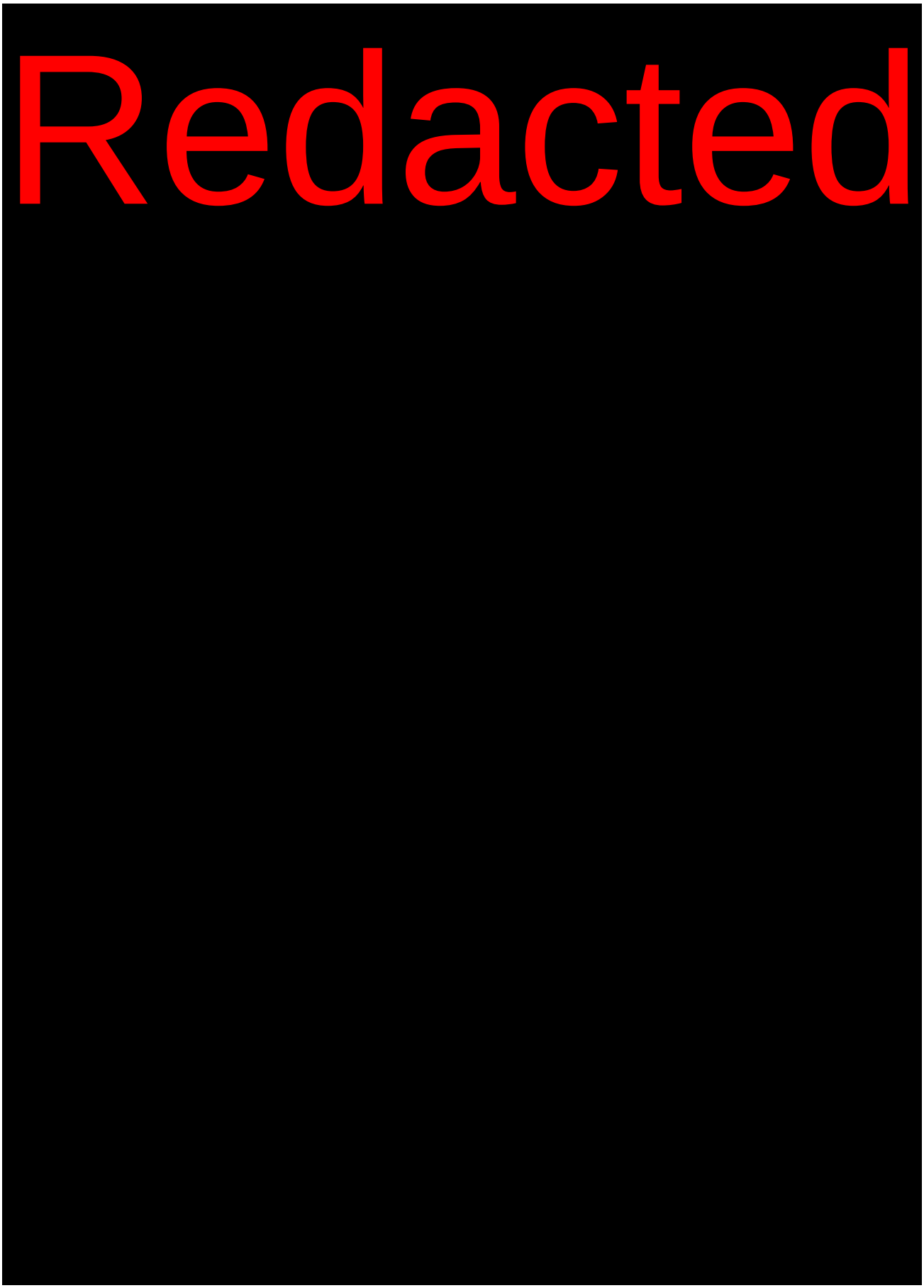
4.2.5 No A&M individuals who have worked on the prior instruction or are outside of the project team have, or have had, access to the Laptop, Dedicated Media or derived data held by A&M.

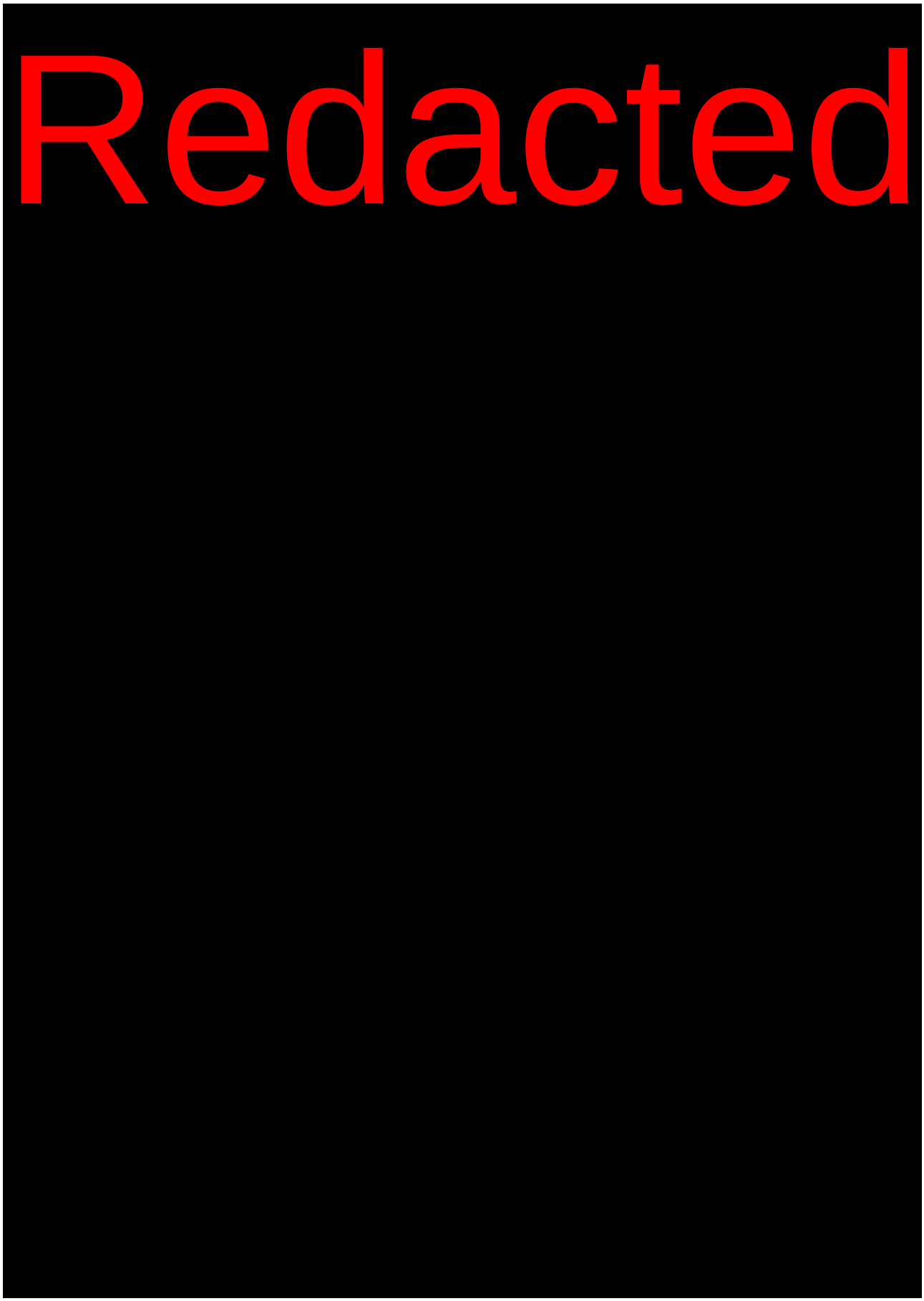

Redacted

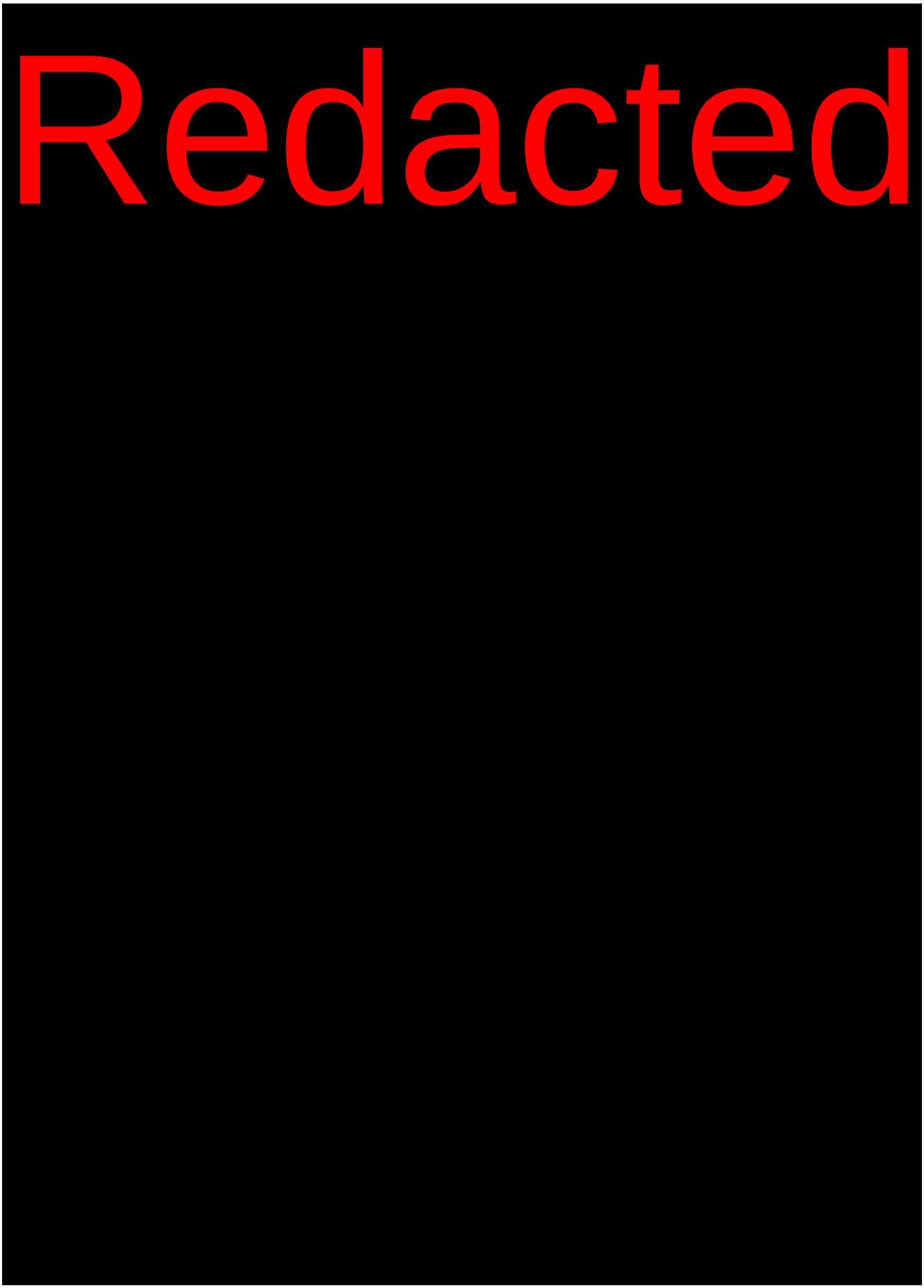

Redacted

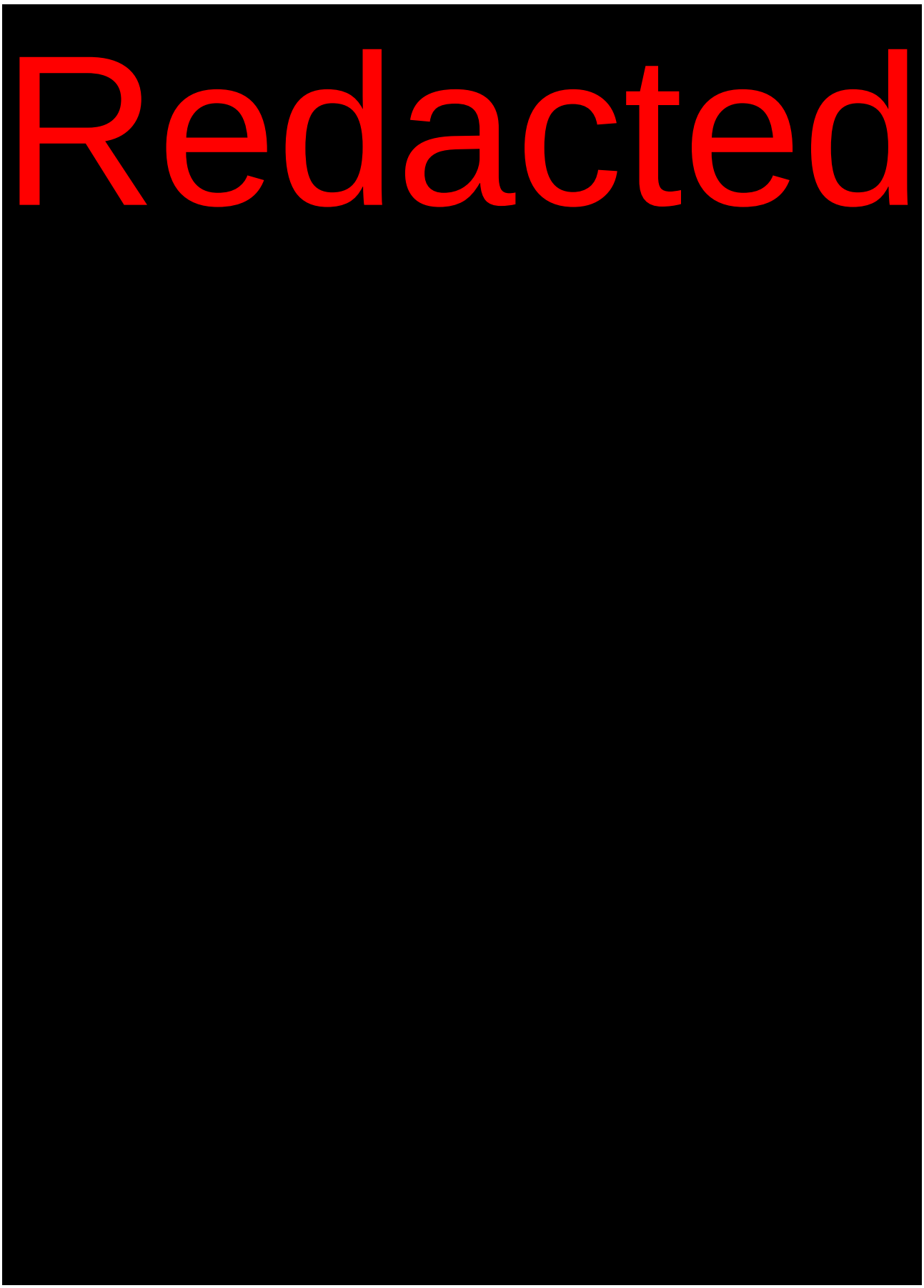

Redacted

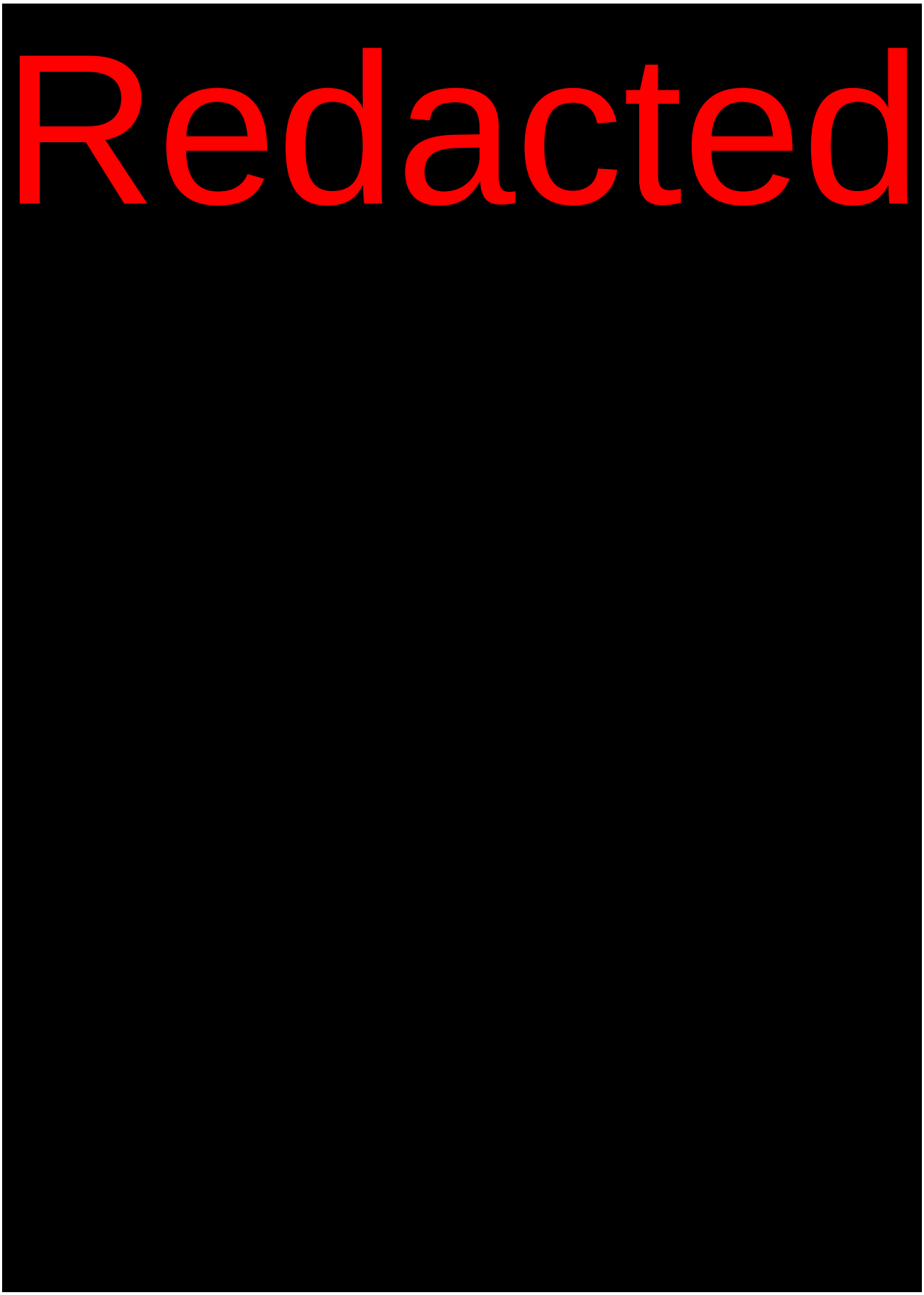

Redacted


Redacted


Redacted


Redacted


Redacted


Redacted

7.1.2 All references to the Forensic Tools refer to the versions specified in 7.1.1 above.

7.1.3 By processing the Laptop Forensic Image using the Forensic Tools it has enabled me to parse, identify and analyse forensic artefacts, which has enabled me to reach the conclusions that I have in this report.

Redacted

8.1.7 The Windows user profile NdR was found to be password protected.

Redacted

8.1.12 All dates and times provided hereafter are in UTC format.

Redacted

8.2 CCleaner

8.2.1 My analysis of the Laptop Forensic Image identified that the CCleaner application is installed on the Laptop in the following location:

i) C:\Program Files\CCleaner\CCleaner.exe

8.2.2 To analyse the CCleaner activity, the User Assist entry within the NTUSER.DAT file was parsed using the Forensic Tools. Details of the NTUSER.DAT file which was analysed to extract the User Assist artefacts have been provided in the table below:

Name	Date Created	Date Modified	Date Accessed	Path	User Assist Location
NTUSER.DAT	10/11/2019 16:05	27/01/2020 05:22	27/01/2020 05:22	C:\Users\NdR\NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

8.2.3 The following User Assist information that was identified in the NTUSER.dat and is relevant to the issues raised in my Instructions (Section 1.2.4 (ii) and (v)) has been provided in the table below.

Windows User Profile	Software	Last Run Date/Time
NdR	CCleaner64.exe	31/01/2020 10:48:03

8.2.4 The above table reports that the CCleaner application was run on 31/01/2020 at 10:48:03 on the Windows user profile NdR.

8.2.5 The following folders were identified on the Laptop Forensic Image:

Folder Name	Date Created	Date Modified	Date Accessed	Z Folders within folder	Z Files within folder
3590F75ABA9E485486C100C1A9D4FF06ZZ.ZZZ.....Z.ZZZ	31/01/2020 10:59:01	31/01/2020 11:02:03	31/01/2020 11:02:03	190	47,466
3590F75ABA9E485486C100C1A9D4FF06ZZZZZZ....Z....Z	31/01/2020 10:55:16	31/01/2020 10:59:00	31/01/2020 10:59:00	249	62,499

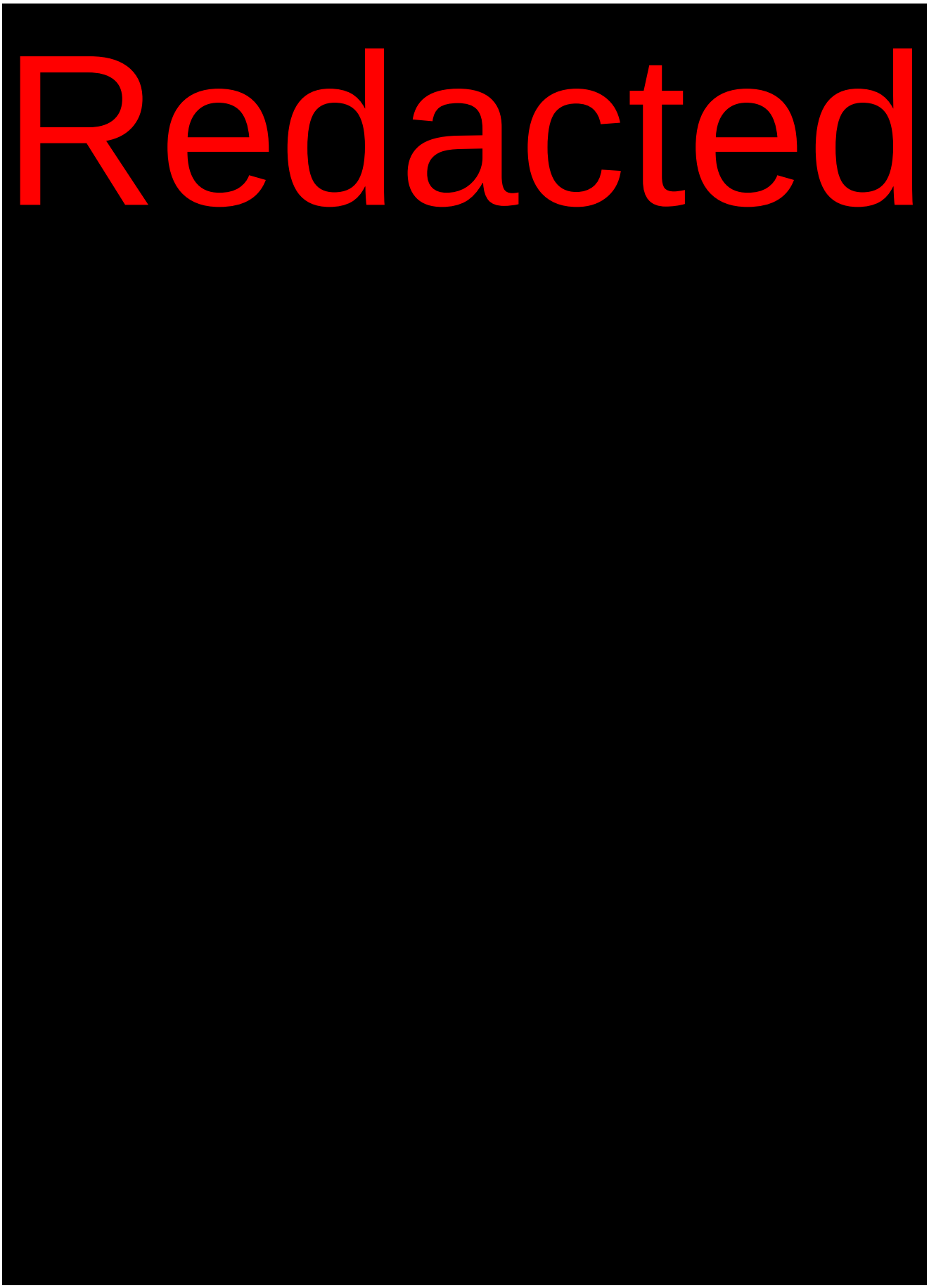
8.2.6 The folders identified on the Laptop Forensic Image which have been provided in the table above are indicative of CCleaner being run using the drive wiper feature (see Section 6.8).

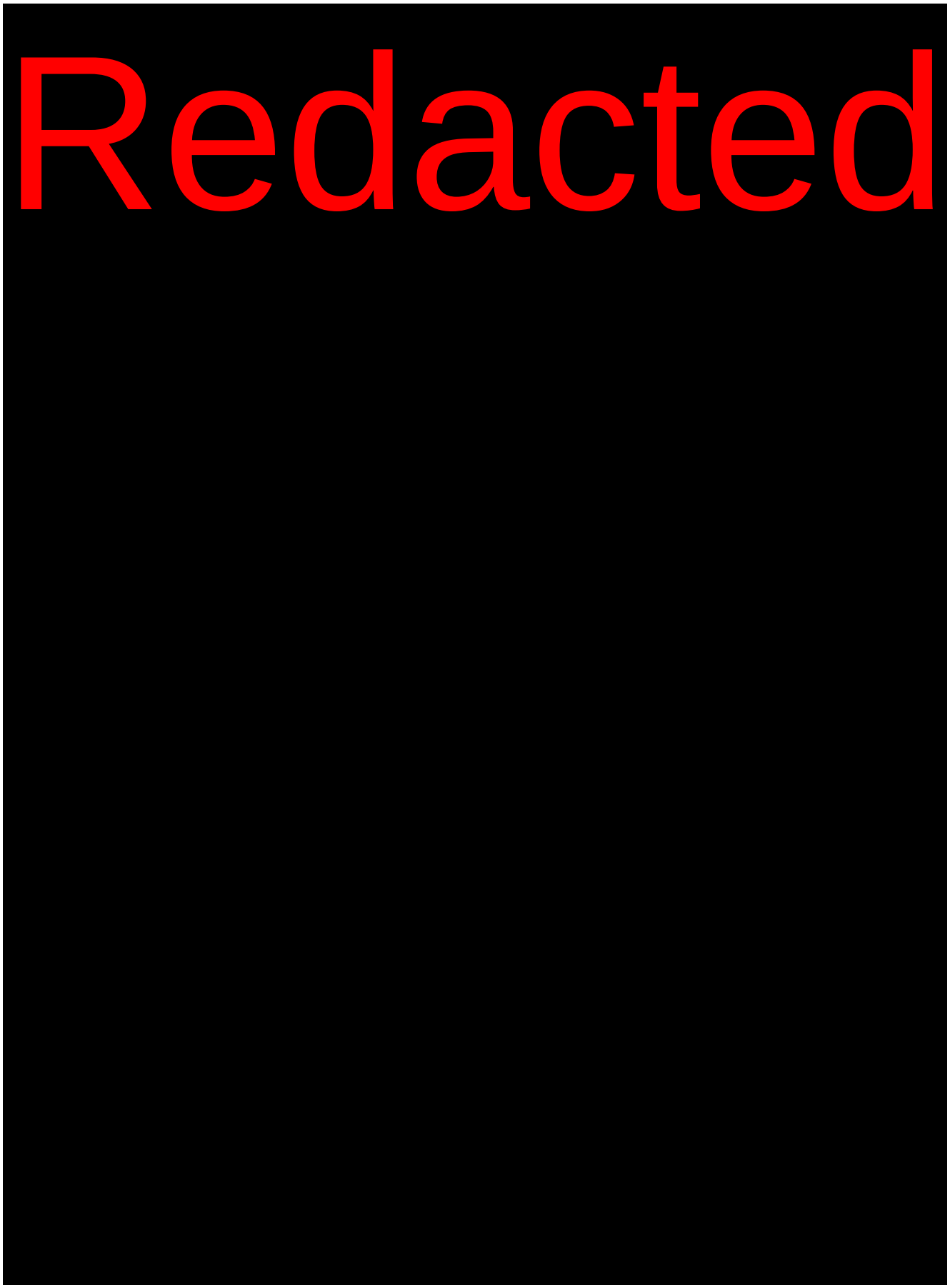
8.2.7 The dates and times provided in the table above are associated with the times that CCleaner created, modified, and last accessed these files and folders. It is not possible to determine the original file and folder names of the files and folders that have been wiped.

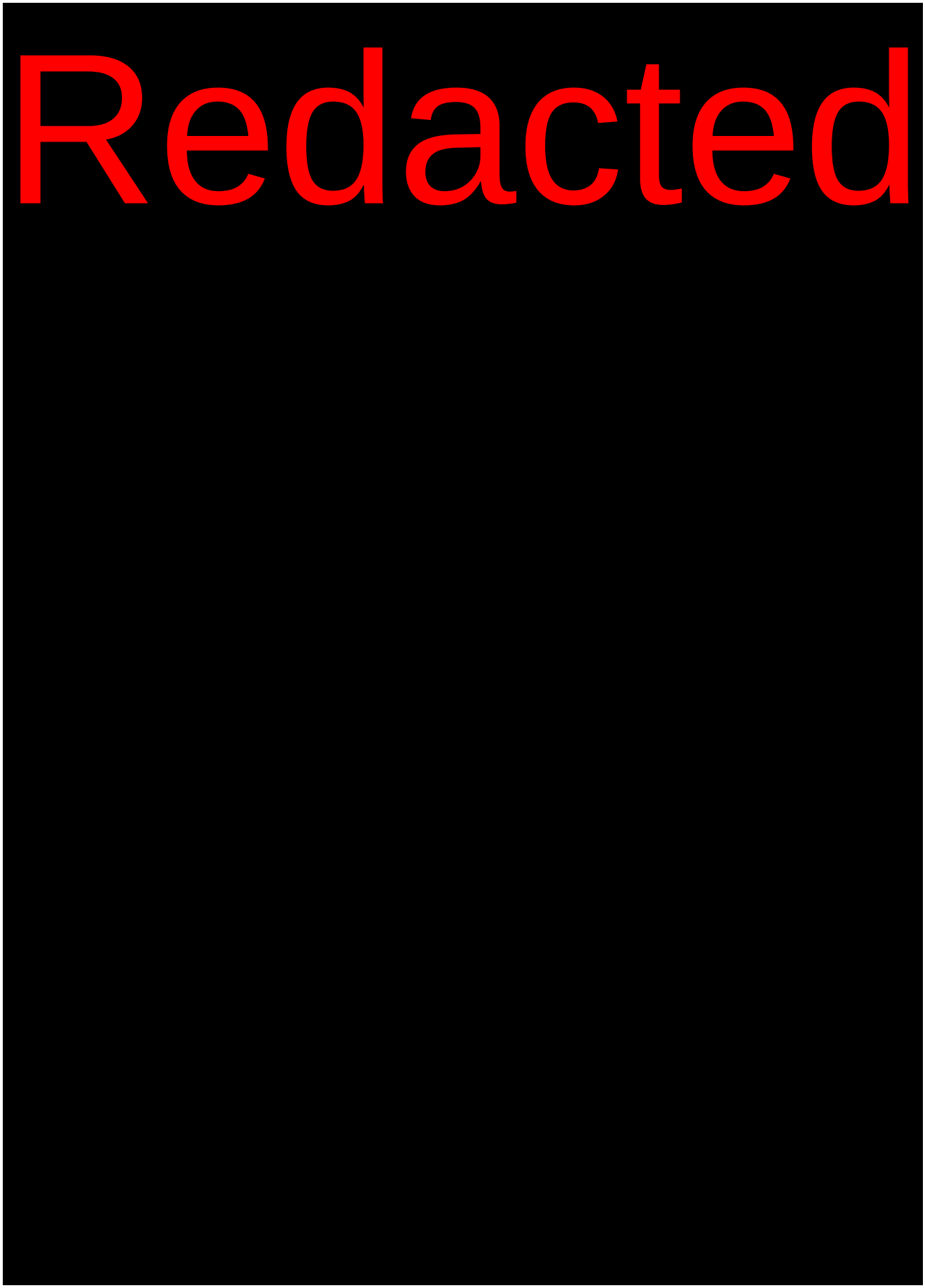
8.2.8 CCleaner has an option to save configuration setting files that report the user settings which are used when the application is run. These files have not been identified on the Laptop Forensic Image and I have not been able to conduct a live examination (see Section 8.1) to see if the option to save configuration files is enabled. I therefore cannot confirm which settings were used when the application was run on the Laptop.

8.2.9 CCleaner can erase traces of user activities; therefore, it is possible that artefacts which were previously stored on the Laptop that would have been relevant to my analysis are no longer present on the Laptop and therefore could not be identified on the Laptop Forensic Image. I have only been able to analyse forensic artefacts that are currently on the Laptop Forensic Image.

8.2.10 The CCleaner artefacts were analysed using multiple Forensic Tools to verify the results of my analysis.


Redacted


Redacted


Redacted

8.5.6 The Jump Lists that have been extracted from the Automatic Destination and Custom Destination files that are relevant to the issues raised in my Instructions (Section 1.2.4 (ii) and (v)) have been provided in the table below.

#	Application	Accessed Target File	Volume Name	Logical Volume Serial Number	Access Count	Target File Created	Target File Last Modified	Target File Last Accessed
1	WinRAR	C:\Users\NdR\Downloads\Compressed\smm@milopc.com_UPDATE24JAN.rar	Windows	0C137B20	1	31/01/2020 08:43:25	31/01/2020 09:39:53	31/01/2020 09:39:53
2	Windows Quick Access	F:\ADMIN\ADMIN\PASSWORDS.docx	Fortress L3	52FF9F8D	2	14/10/2019 10:15:47	31/01/2020 10:50:50	31/01/2020 10:50:50
3	Microsoft Word	F:\ADMIN\ADMIN\PASSWORDS.docx	Fortress L3	52FF9F8D	2	14/10/2019 10:15:47	10/01/2020 20:16:52	10/01/2020 20:16:52

8.5.7 In respect to entry #3 in the table above as an example:

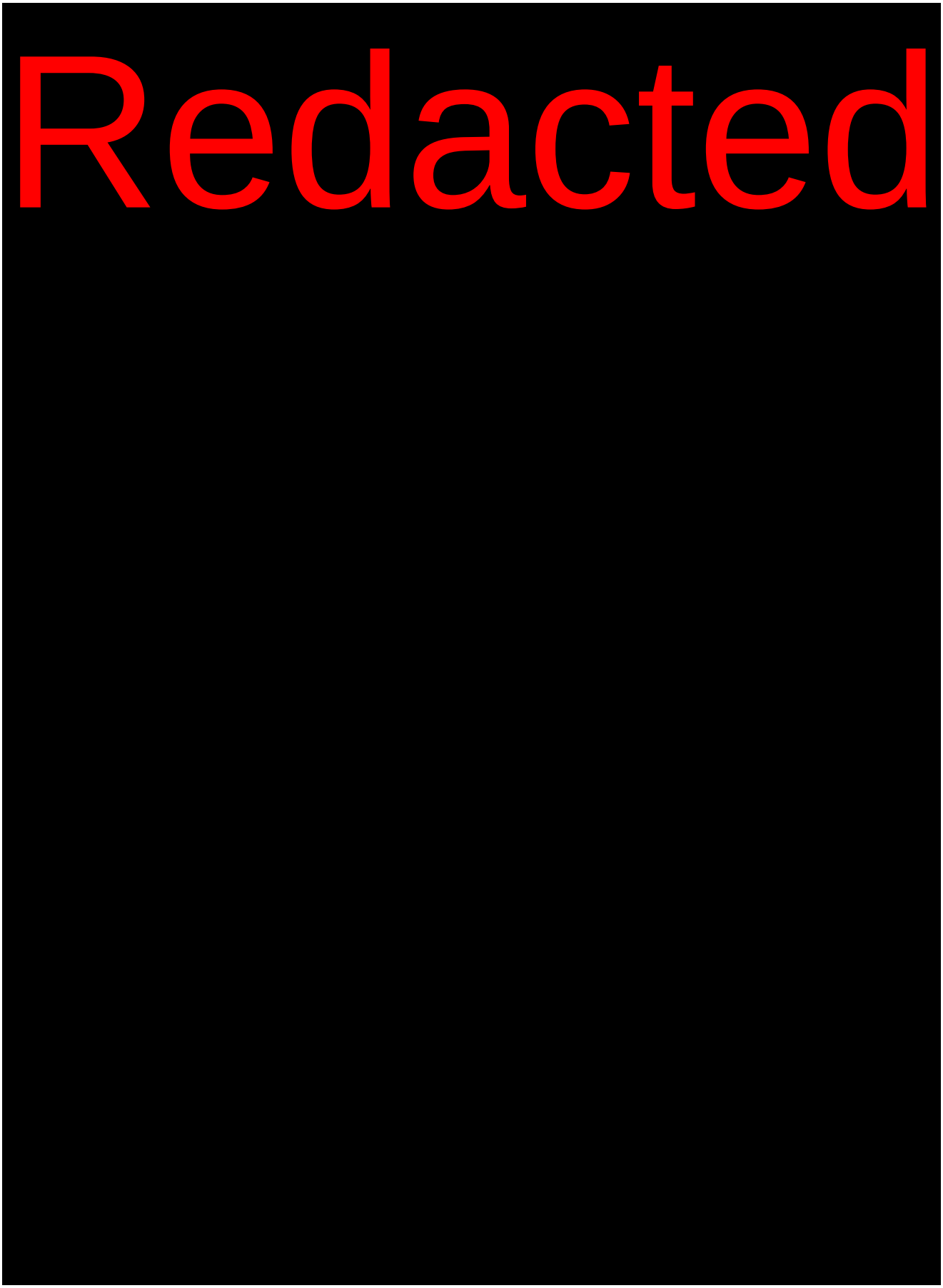
i) The Microsoft Word application was used to access the Target File "F:\ADMIN\ADMIN\PASSWORDS.docx".

ii) At the time it was accessed, the Target File was stored on volume F: with the name "Fortress L3[22]" and serial number 52FF9F8D. A Fortress L3 Device is an

Aegis Fortress L3 Device manufactured by Apricorn which utilises a keypad for encryption and decryption.

iii) I note that this Apricorn Aegis Fortress L3 Device is a different Aegis device to the Aegis Device referenced in my Instructions (Section 1.2.4 (v)) which is currently held by the Claimant.

iv) The Target File is reported to be created on that volume, accessed, and modified at the dates shown in the columns: Target File Created, Target File Last Modified, and Target File Last Accessed.


Redacted

Redacted

8.7 USB Artefacts

8.7.1 When a USB device is inserted into a Windows computer, the Windows Registry records the event and other associated information. For example:

i) Name of the USB device

ii) Serial Number

iii) Last connected date

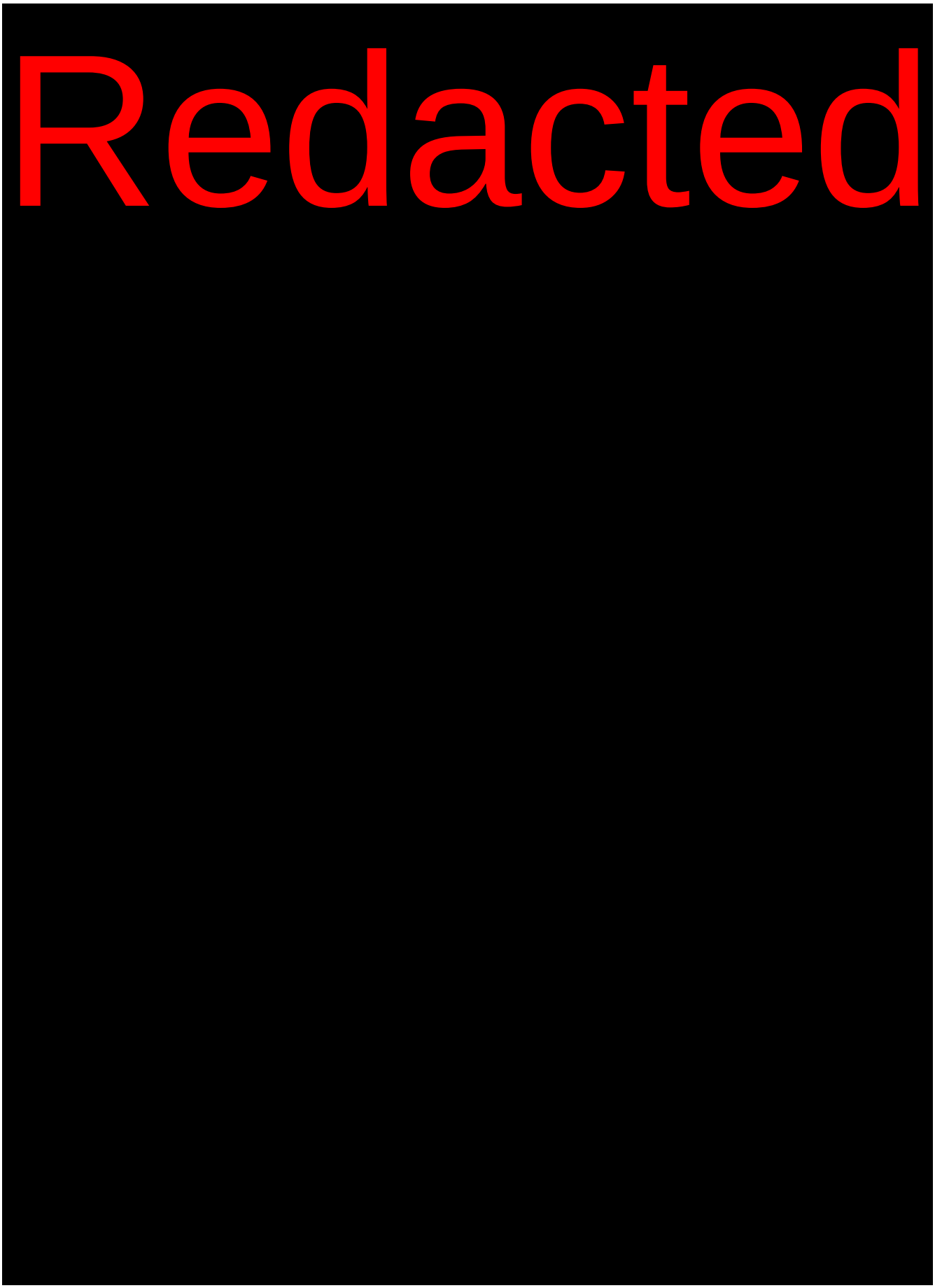
iv) Last removed date/time

v) First connected date/time

8.7.2 Details of the USB artefacts that have been extracted from the Windows Registry on the Laptop Forensic Image and are relevant to the issues raised in my Instructions (Section 1.2.4 (ii) and (v)) have been provided in the table below:

Device Name	Serial Number	Last Connected	Last Removed	First Connected
Apricorn Fortress L3 USB Device	121700000096	31/01/2020 10:26:05	31/01/2020 10:51:38	11/11/2019 13:14:44

Redacted


Redacted

8.9.3 **USB Activity**

8.9.4 USB device information is stored within Windows Event logs, in addition to being recorded within the Windows Registry (see Section 8.7).

8.9.5 Upon examining the event log named "Microsoft-Windows-Partition%4Diagnostic.evtx", I was able to ascertain information related to USB device activity.

8.9.6 The below table details information identified in the "Microsoft-Windows-Partition%4Diagnostic.evtx" event log file that is relevant to the issues raised in my Instructions (Section 1.2.4 (ii) and (v)). This table shows the following details:

i) **Manufacturer** – the manufacturer of the USB device

ii) **Model** – the specific model type of the USB device

iii) **Serial Number** – the serial number of the physical USB device

iv) **Volume Serial Number** – the serial number assigned to each volume on the USB device.

v) **Date/Time** – the date and time associated with the event

vi) **Action** – this shows if the USB device was connected or disconnected at the date and time of event

#	Manufacturer	Model	Serial Number	Volume Serial Number	Date/Time	Action
1	Apricorn	Fortress L3	121700000096	52FF9F8D	31/01/2020 10:26:05	Connected
2	Apricorn	Fortress L3	121700000096	52FF9F8D	31/01/2020 10:51:38	Disconnected

8.9.10 **Logon Activity**

8.9.11 Upon examining the event log named "Security.evtx", I was able to ascertain information related to user logon activity on the computer file that is relevant to the issues raised in my Instructions (Section 1.2.4 (ii) and (v)).

8.9.12 The below table shows that the user with the name "NdR" was logged on at two separate times on 31 January 2020. These events occurred at 07:26am and 10:25am. The login type for these logons is "Interactive". An interactive login is one which is performed on the computer itself i.e. at the keyword.

Record	Created Date/Time (UTC)	Event Description Summary	Logon Type	Target Username
1	31/01/2020 07:26:53	An account was successfully logged on.	2-Interactive	NdR
2	31/01/2020 10:25:06	An account was successfully logged on.	2-Interactive	NdR

8.9.13 I have reviewed all logon events and have not identified any logons that were user related, and which were not defined as "Interactive". Any such other logon events can include remote logons or logons via networked computers.

8.9.14 **Date and Time Settings**

8.9.15 Upon examining the event log named "Microsoft-Windows-Time-Service%4Operational.evtx", I was able to ascertain information related to the date and time and time settings on the computer that is relevant to the issues raised in my Instructions (Section 1.2.4 (vii)).

8.9.16 This event log file shows that the computer has automatically synchronised the date and time with the time.windows.com[24] server (IP Address[25] 51.145.123.29) on 31 January 2020. Logs synchronising with the time.windows.com server begin on 11 November 2019 and end on 31 January 2020.

8.9.17 As an example of the time synchronisation, on 31 January 2020, the log files show the following information which strongly indicate the time settings are accurate at that time.

i) 31/01/2020 03:23:25 – "The time service is now synchronizing the system time with the reference time source **time.windows.com"**

ii) 31/01/2020 03:23:25 – "The W32time service has set the system time to **2020-01-31 03:23:25.20"**

8.9.18 Based upon the time synchronisation logs that I have reviewed, there is evidence to suggest that on the key dates indicated in my report, the time and date of the computer was accurate.

Redacted

[24] time.windows.com is a website hosted by Microsoft that relays the exact date and time information to any computer that communicates with it via the Windows Time service (W32Time). The time synchronisation requires an active internet connection.
[25] An IP (Internet Protocol) address is a numerical identifier assigned to a device that is connected to a network that uses the Internet.

8.10 Malicious Files

8.10.1 In addition to my analysis of Windows Event Logs to determine if malicious remote access took place (see Section 8.9), I also conducted an analysis to identify if malicious files reside on the Laptop Forensic Image.

8.10.2 The Laptop Forensic Image was mounted[26] on a Windows OS and the following virus scanning tools were run over the mounted Laptop Forensic Image:

i) ClamAV[27]

ii) MalwareBytes[28]

8.10.3 The results of these scans did not identify any malicious files or artefacts that suggest unauthorised remote access has been gained to the device.

8.10.4 At the time of my analysis, it was not possible to run a scan for viruses during a live examination (which would typically be more comprehensive) because I could not gain access to the Windows OS as I do not have the password for Windows user profile NdR.

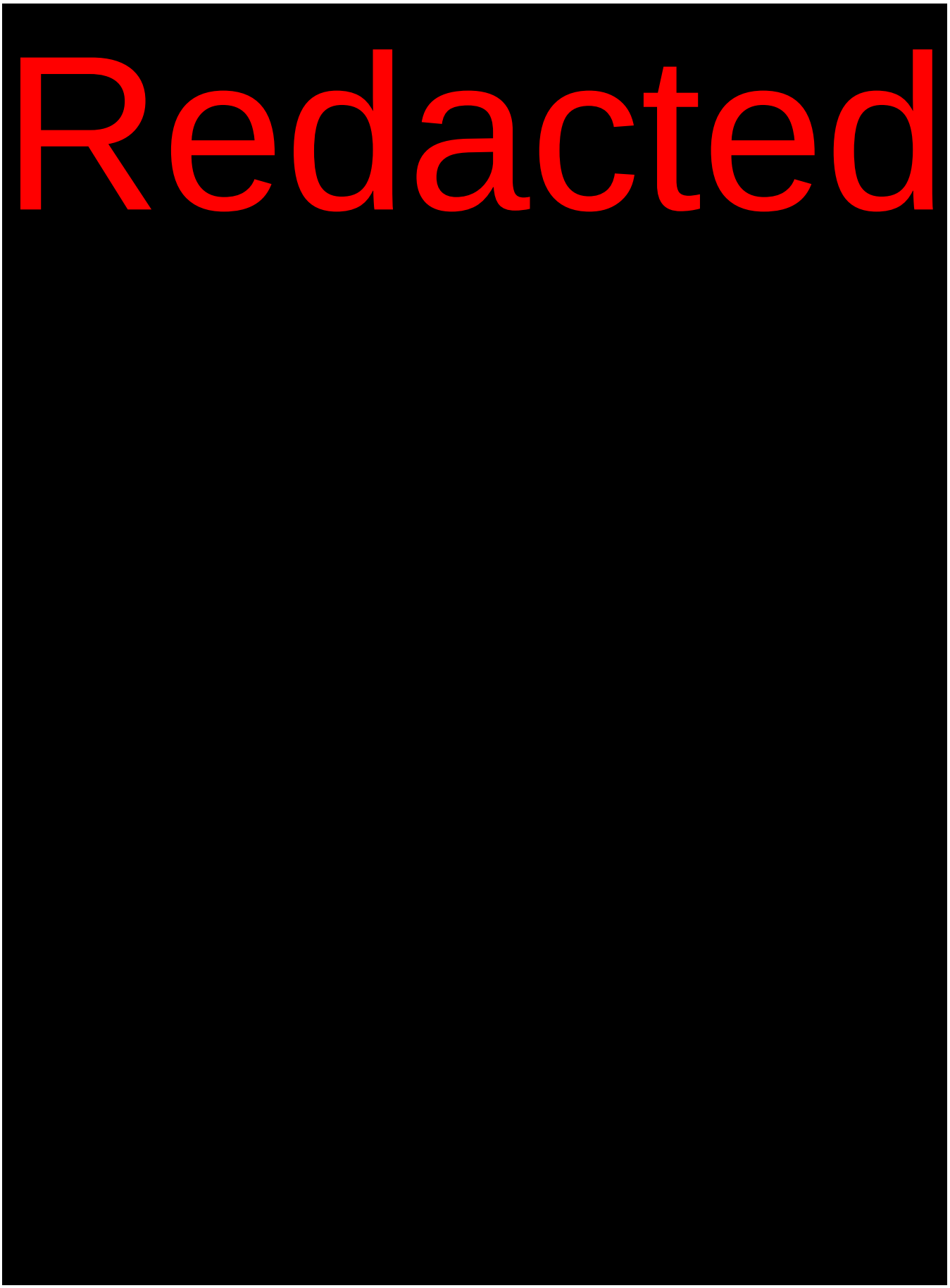
8.10.5 McAfee Virus scanning software was found to be installed on the Laptop. The following logs are indicative that McAfee did not identify any viruses during a live system scan. Please find the logs below:

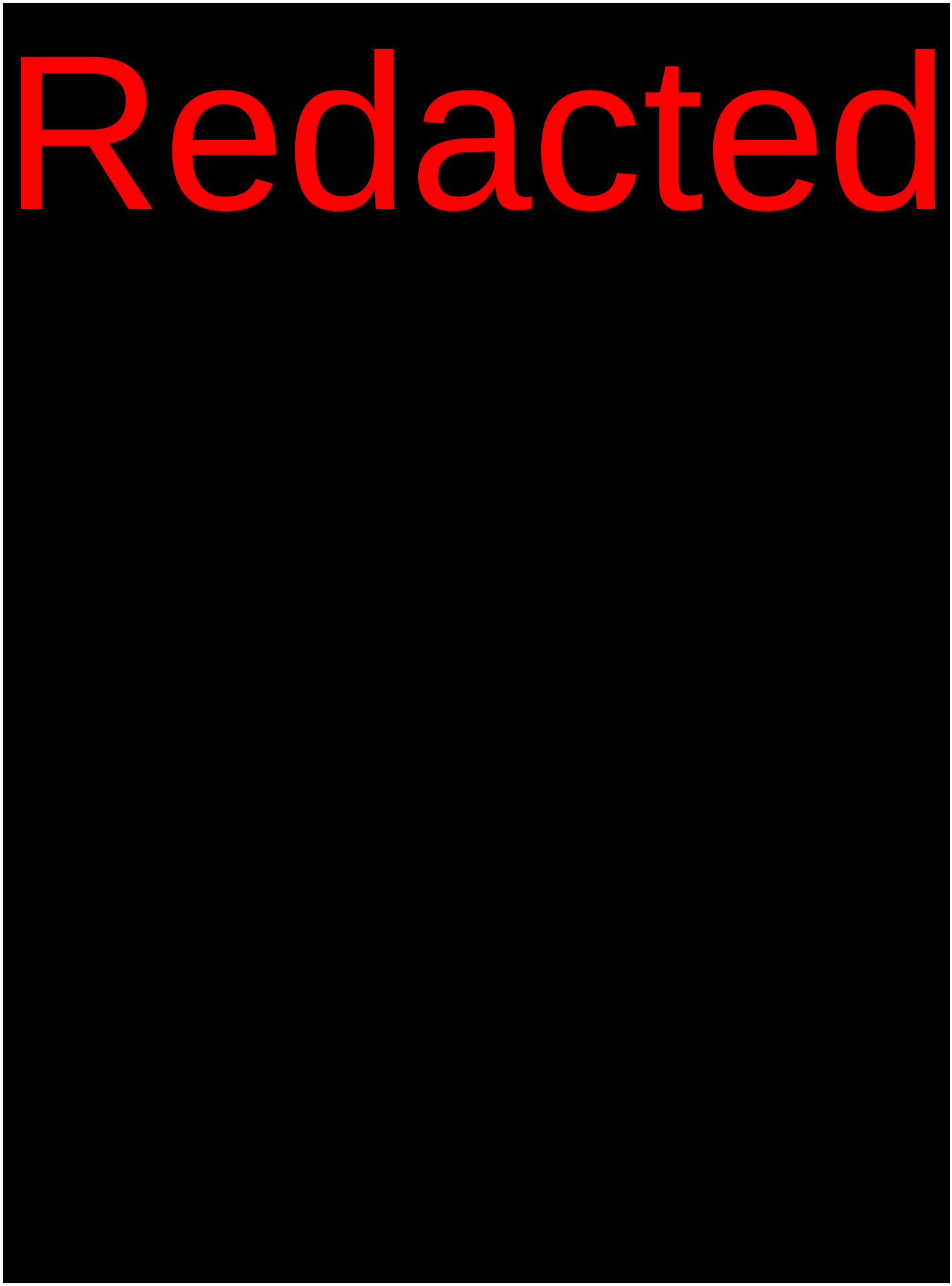
Log Name	Log Detail	Log Date	Full path
VMapLogs.log	MachineID=_{916D75C5-B9D3-41E6-9633-31DE2A8B1E0E} HardwareID=3d4010b837ffdc0d13b4f450047cd755 Posted Viruses=0	31/01/2020 13:20:29	C:\ProgramData\McAfee\VirusScan\Data\VMapLogs.log
VMapLogs.old	MachineID=_{916D75C5-B9D3-41E6-9633-31DE2A8B1E0E} HardwareID=3d4010b837ffdc0d13b4f450047cd755 Posted Viruses=0	30/01/2020 10:56:44	C:\ProgramData\McAfee\VirusScan\Data\VMapLogs.old

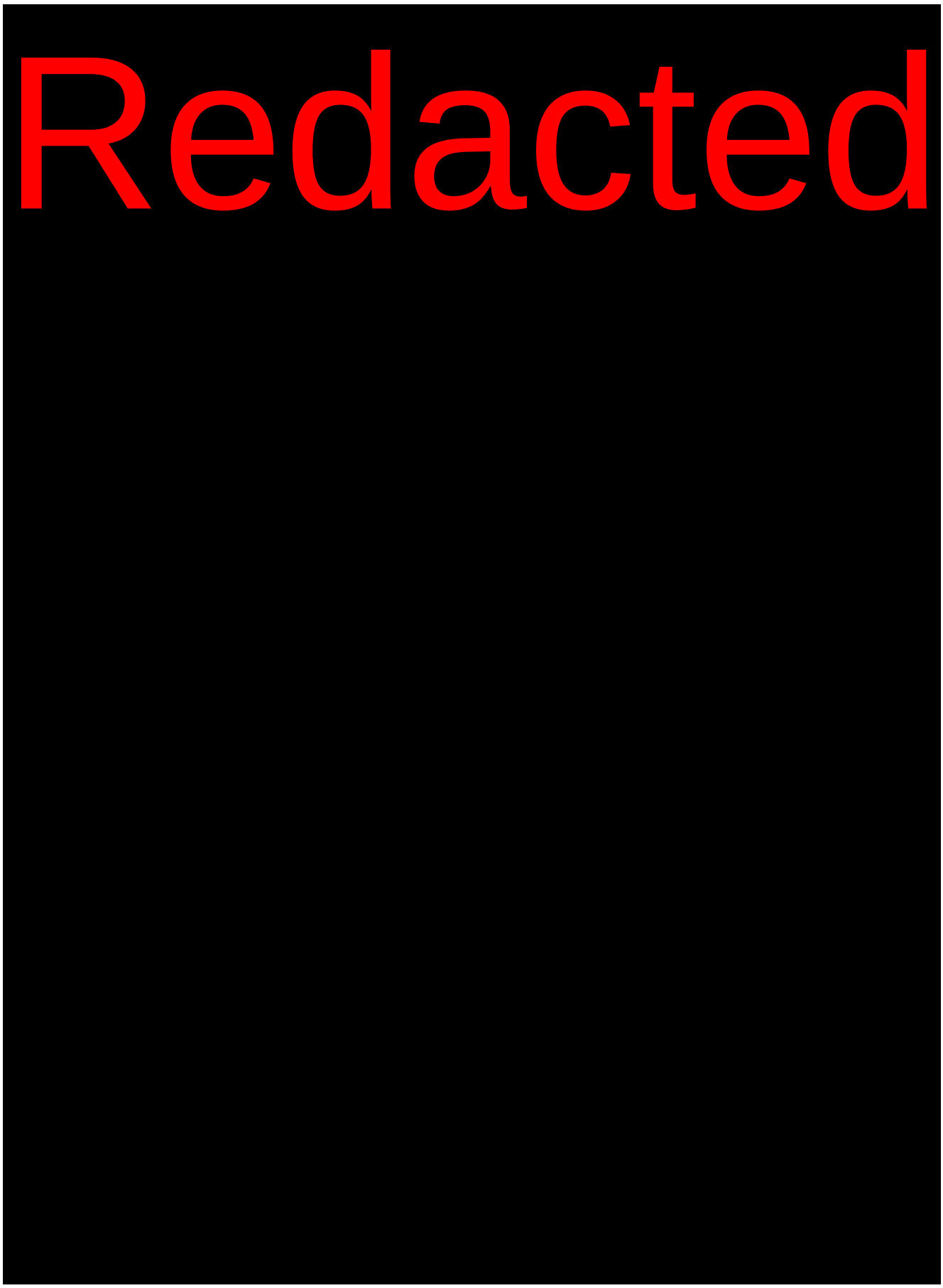
[26] Mounting an image refers to the process of making the contents of an image accessible to the Windows (or other) operating system as if it were a physical disk drive.

[27] ClamAV is an open source anti virus scanner that is currently developed by Cisco's cybersecurity business, Talos.

[28] Malwarebytes is a highly regarded malware removal tool that has been in development since 2006.


Redacted


Redacted


Redacted

8.13 Chronology of Forensic Artefacts

8.13.1 My analysis has identified various forensic artefacts that are relevant to the issues raised in my Instructions (Section 1.2.4 (ii) and (v)). These artefacts have been organised chronologically.

8.13.2 A full Chronology of Forensic Artefacts is exhibited as Exhibit PB2-01.

8.13.3 Set out below is an explanation of the Forensic Artefacts that are detailed Exhibit PB2-01.

8.13.4 **Rows 1 to 4**

8.13.4.1 These rows show that a file named “PASSWORDS.docx” and a folder7named “RECOVERY KEYS” are accessed using Microsoft Word and Windows Explorer. These files and folders are shown as being present on an external volume named “Fortress L3” with serial number “52FF9F8D” (Apricorn Aegis Fortress L3 Device). On 11 November 2019 at 13:14:44, the Apricorn Fortress L3 USB Device is inserted to the Laptop. On 10 January 2020 at 20:16:52 the file named “PASSWORDS.docx” has the last modified/accessed dates updated.

#	Date	Forensic Artefact	Application	Type	Activity / Event Description
1	14/10/2019 10:15:47	Jump Lists	Windows Explorer/Microsoft Word	Password File Created on F: Volume	"F:\ADMIN\ADMIN\PASSWORDS.docx" Date Created on Apricorn Aegis Fortress L3 USB Device
2	14/10/2019 10:15:47	Microsoft Office Backstage Items	Microsoft Word	Recovery Keys Folder on F: Volume	"F:\ADMIN\ADMIN\RECOVERY KEYS" Last Modified Date on Apricorn Aegis Fortress L3 USB Device
3	11/11/2019 13:14:44	USB Artefacts (Windows Registry)	USB Device Connected	Apricorn Aegis Fortress L3 USB Device is Connected	Apricorn Aegis Fortress L3 USB Device is Connected
4	10/01/2020 20:16:52	Jump Lists	Windows Explorer/Microsoft Word	Password File Last Accessed/Modified on F: Volume	"F:\ADMIN\ADMIN\PASSWORDS.docx" Last Accessed/Modified on Apricorn Aegis Fortress L3 USB Device


Redacted

8.13.7 **Row 18**

8.13.7.1 These rows show that on 31 January 2020 at 10:48:03 the CCleaner application is opened (see Section 8.2)

#	Date	Forensic Artefact	Application	Type	Activity / Event Description
18	31/01/2020 10:48:03	User Assist Windows Registry	CCleaner	CCleaner	CCleaner last run date

8.13.8 **Rows 19 to 22**

8.13.8.1 These rows show that on the 31 January 2020 at 10:48:57 the file “F:\ADMIN\ADMIN\PASSWORDS.docx” is accessed using Microsoft Word. The Last Modified and Accessed dates of the file are updated on Apricorn Fortress L3 USB Device and Microsoft Word is then closed. The Apricorn Fortress L3 USB Device is removed from the Laptop (see Sections 8.4, 8.6 and 8.7).

#	Date	Forensic Artefact	Application	Type	Activity / Event Description
19	31/01/2020 10:48:57	Windows Timeline	Microsoft Word	Accessing Password File	Microsoft Word application **Start Time.** File "F:\ADMIN\ADMIN\PASSWORDS.docx" is open within the application. (The application was open/in focus)
20	31/01/2020 10:50:50	Jump Lists/LNK Files	Windows Quick Access	Password File Last Modified Date	"F:\ADMIN\ADMIN\PASSWORDS.docx" Last Accessed/Modified Date
21	31/01/2020 10:50:54	Windows Timeline	Microsoft Word	Application End Time	Microsoft Word application **End Time**
22	31/01/2020 10:51:38	USB Artefacts (Windows Registry) and Windows Event Logs	USB Device Removed	Apricorn Aegis Fortress L3 USB Device is removed (F:)	Apricorn Aegis Fortress L3 USB Device is removed (F:)

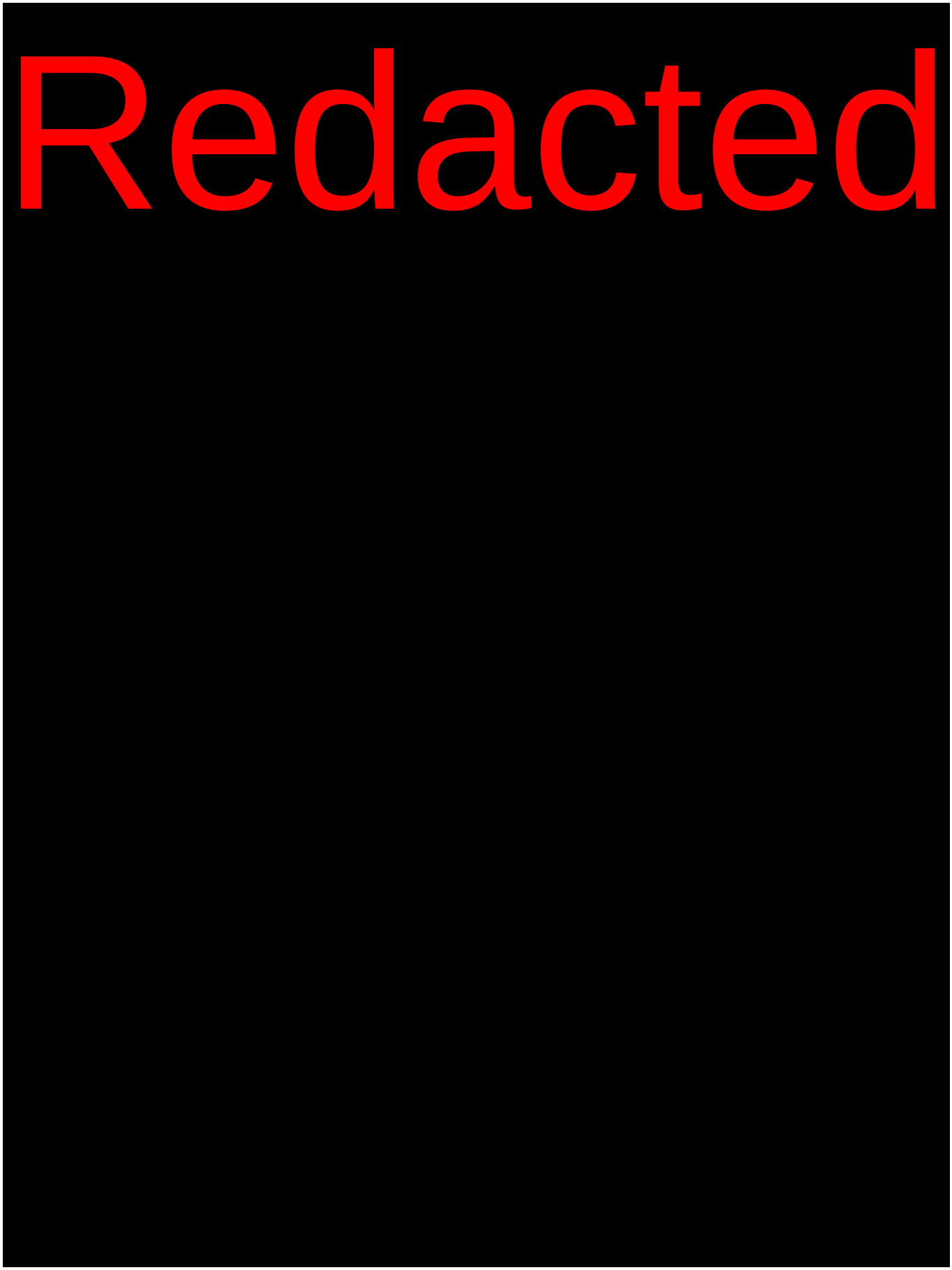
8.13.9 **Rows 23 to 26**

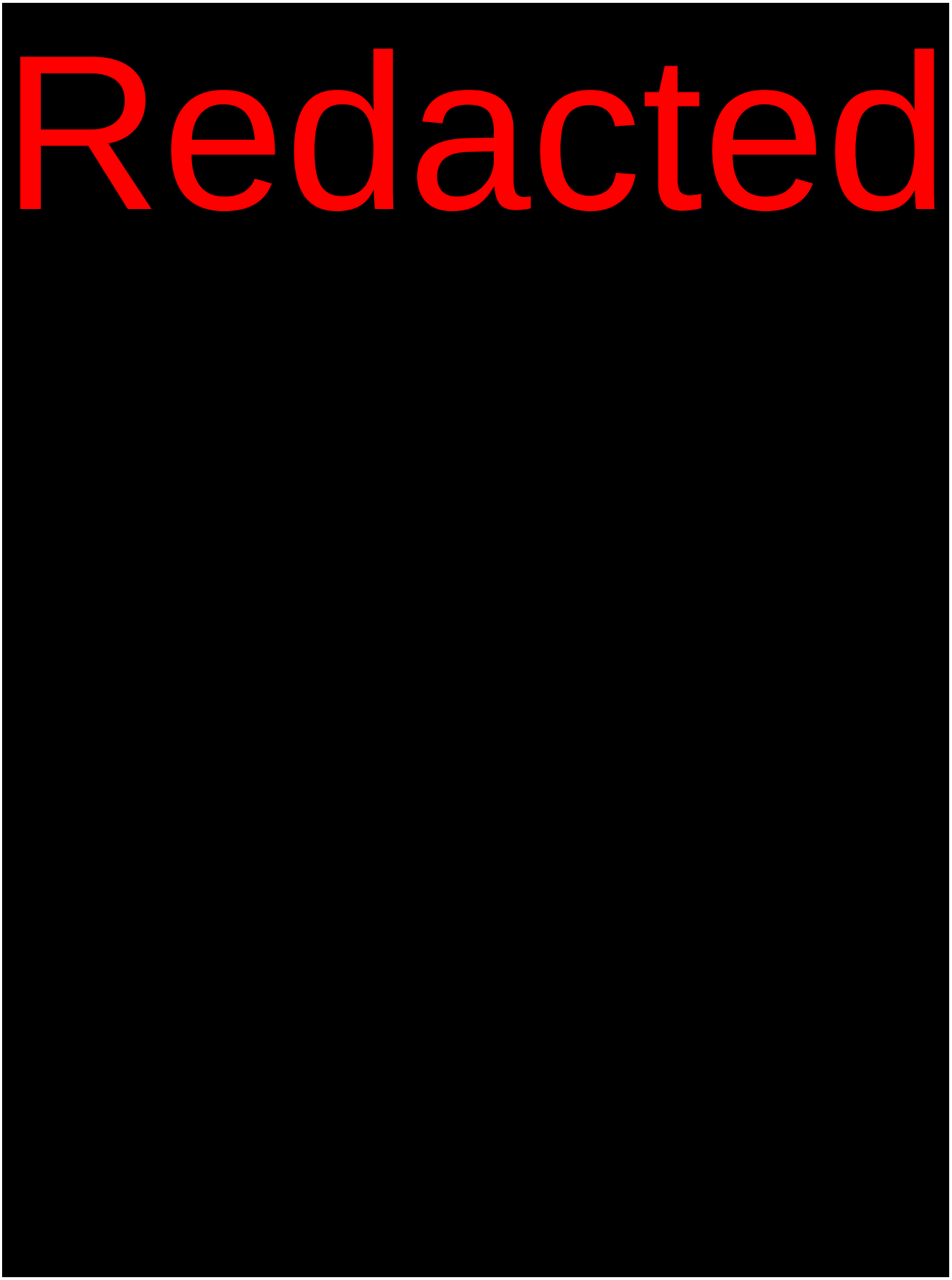
8.13.9.1 These rows show that on 31 January 2020 at 10:55:16 and 10:59:01 the created dates for the CCleaner Z files are updated. At 10:59:00 and 11:02:03 the last accessed/modified dates of these files are also. This is indictive of the CCleaner drive wiper setting being used (see Sections 8.2 and 8.4).

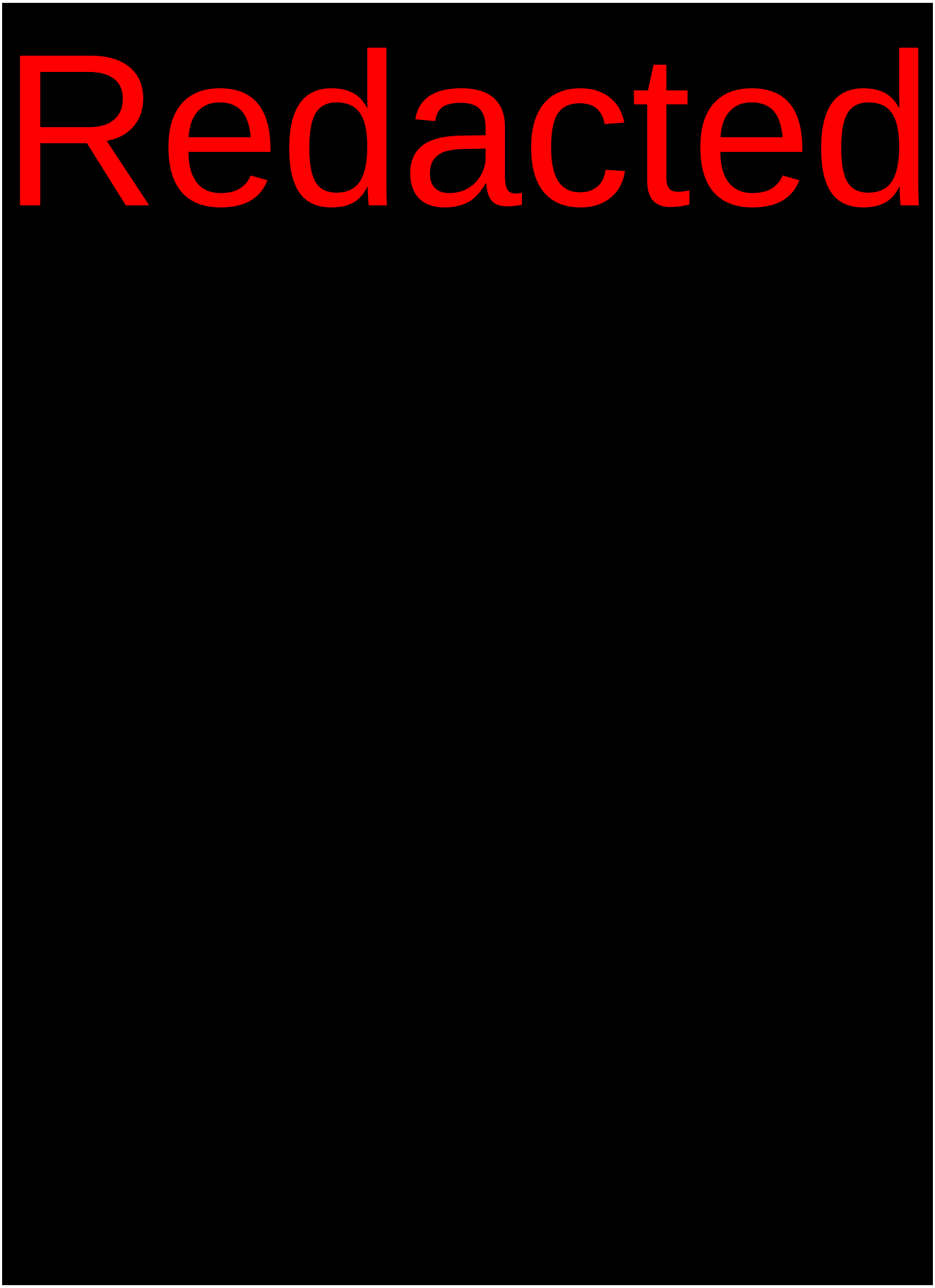
#	Date	Forensic Artefact	Application	Type	Activity / Event Description
23	31/01/2020 10:55:16	Folders/Files	CCleaner	CCleaner File Created Date	CCleaner drive wiping Z file Date Created
24	31/01/2020 10:59:00	Folders/Files	CCleaner	CCleaner File Last Accessed/Modified Data	CCleaner drive wiping Z file Last accessed/Modified date
25	31/01/2020 10:59:01	Folders/Files	CCleaner	CCleaner File Created Date	CCleaner drive wiping Z file Date Created
26	31/01/2020 11:02:03	Folders/Files	CCleaner	CCleaner File Last Accessed/Modified Data	CCleaner drive wiping Z file Last accessed/Modified date

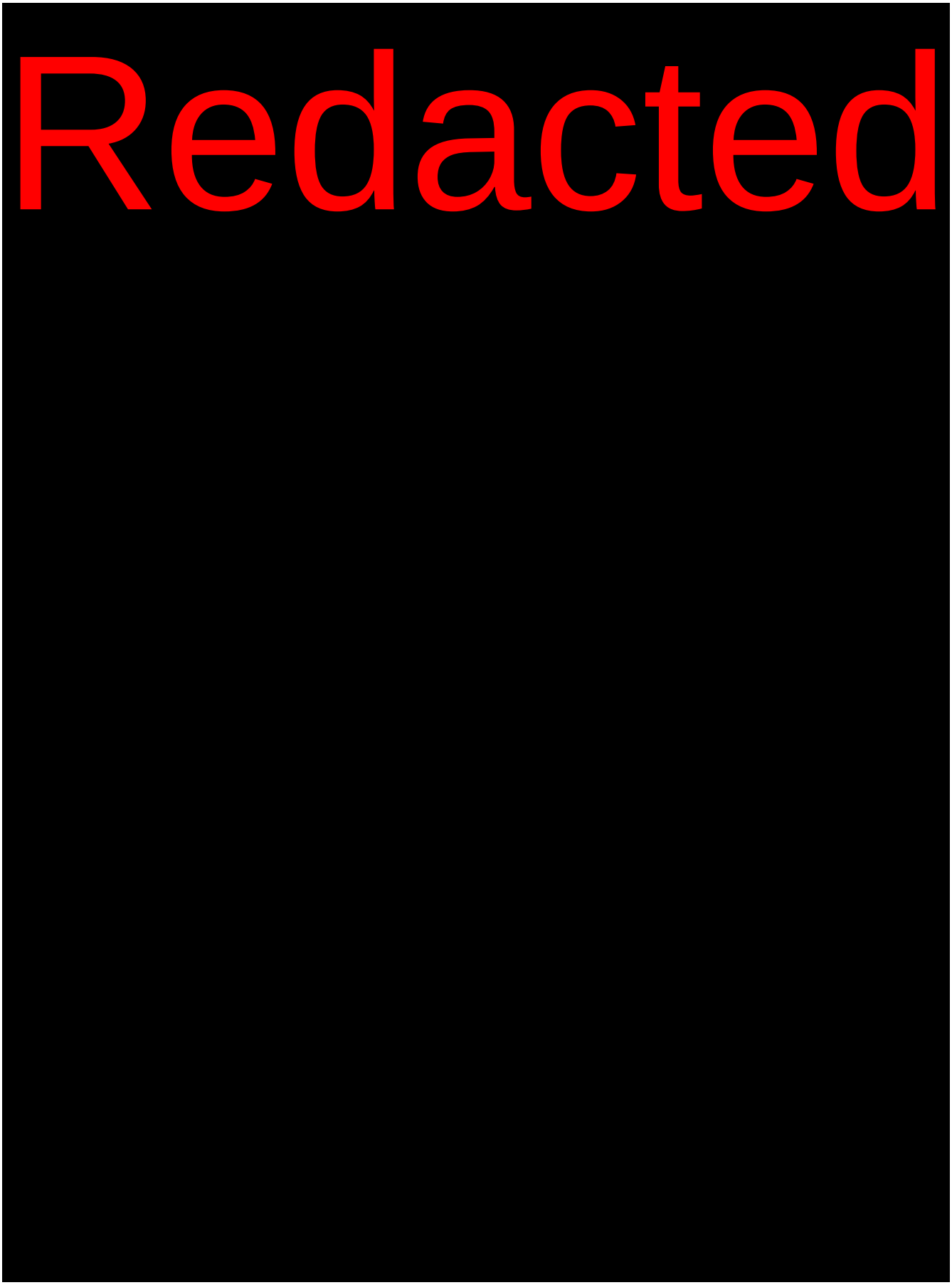

Redacted


Redacted


Redacted


Redacted


Redacted


Redacted

11 Expert Declaration

11.1.1 I, Phil Beckett, declare that:

i) I understand that my duty in providing written reports and giving evidence is to help the Court, and that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied and will continue to comply with my duty.

ii) I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.

iii) I know of no conflict of interest of any kind, other than any which I have disclosed in my report.

iv) I do not consider that any interest which I have disclosed affects my suitability as an expert witness on any issues on which I have given evidence.

v) I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affect my answers to points iii) and iv) above.

vi) I have shown the sources of all information I have used.

vii) I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.

viii) I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.

ix) I have not, without forming an independent view, included or excluded anything which has been suggested to me by others, including my instructing lawyers.

x) I will notify those instructing me immediately and confirm in writing if, for any reason, my existing report requires any correction or qualification.

xi) I understand that:

a. my report will form the evidence to be given under oath or affirmation;

b. questions may be put to me in writing for the purposes of clarifying my report and that my answers shall be treated as part of my report and covered by my statement of truth;

c. the court may at any stage direct a discussion to take place between experts for the purpose of identifying and discussing the expert issues in the proceedings, where possible reaching an agreed opinion on those issues and identifying what action, if any, may be taken to resolve any of the outstanding issues between the parties;

d. the court may direct that following a discussion between the experts that a statement should be prepared showing those issues which are agreed, and those issues which are not agreed, together with a summary of the reasons for disagreeing;

e. I may be required to attend court to be cross-examined on my report by a cross-examiner assisted by an expert;

f. I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.

xii) I have read Part 35 of the Civil Procedure Rules, the accompanying practice direction and the Guidance for the instruction of experts in civil claims and I have complied with their requirements.

xiii) I am aware of the practice direction on pre-action conduct and I have acted in accordance with the Code of Practice for Experts.

Statement of Truth

ii) I confirm that I have made clear which facts and matters referred to in this Report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Phil Beckett

9 February 2024

Phil Beckett
Managing Director

Alvarez & Marsal

Alvarez & Marsal Disputes and Investigations, LLP
Park House, 16-18 Finsbury Circus, London EC2M 7EB
pbeckett@alvarezandmarsal.com

Employment

- Alvarez & Marsal
- Proven Legal Technologies
- Navigant Consulting
- BDO Stoy Hayward LLP
- Andersen

Professional qualifications

- FCCA (Fellow of the Association of Chartered Certified Accountants)
- CFE (Certified Fraud Examiner)
- MBCS (Member of the British Computer Society)

Education

- B.Sc. (Hons) Computing & Management
- M.SC Forensic Computing
- LLM Computer and Communications Law

Phil Beckett, a Managing Director, Leader of A&M's European & Middle East Disputes and Investigations practice and leader of A&M's Global Forensic Technology team, brings more than 20 years of experience in forensic technology engagements, advising clients on forensic investigations of digital evidence, the interrogation of complex data sets and the disclosure of electronic documents. He was named Who's Who Legal's Investigations Digital Forensic Expert of the Year in 2017 & 2018 and the Forensic Technology team are listed in Band One within Chambers and Partners UK-wide eDiscovery Rankings.

He has worked with global clients across a wide range of sectors, including oil & gas, financial services, IT software/hardware, automotive, electronic equipment, power generation, chemicals, music and entertainment, defence and aviation, engineering, construction, manufacturing, professional services and healthcare. Mr. Beckett has acted as an IT Forensics Expert and given written testimony.

Mr. Beckett has led anti-bribery investigations, kickback investigations, IP theft cases, employment disputes, fraud investigations, cartel/anti-trust investigations, compliance review exercises, and supported commercial litigation and international arbitration. Many of these cases have been cross-border, requiring close monitoring of data protection and privacy legislation and the appropriate use of technology.

Mr. Beckett was previously a Partner at Proven Legal Technologies and a Managing Director at Navigant leading their European Forensic Technology Practice for seven years where his clients included major internationally-listed companies as well as large privately owned or private equity-funded businesses.

Mr. Beckett earned a bachelor's degree in computing and management from the Loughborough University, a master's degree in forensic computing from Cranfield University and is a Fellow of the Association of Chartered Certified Accountants (ACCA), winning the ACCA Gold Medal when he qualified in 2001. He is a Certified Fraud Examiner (CFE) and lectures regularly on information governance and digital investigations

Expert witness

- Acted as an expert witness in a case between parties who were in dispute over how investments had been made in respect of a sovereign wealth fund. The work involved analysing certain artefacts present on a computer in order to determine the integrity of the document that the artefacts related to.
- Acted as a joint expert in a case related to an alleged copyright infringement in respect to the copying of source code for a data analysis program. The work involved comparing two sets of source code to determine any findings that would be indicative of it being copied or developed independently. In addition, the expert report detailed the significance that any finding had in respect of the entire application.
- Acted as an expert witness in a case between parties who had engaged in a series of business transactions, producing a report based on the integrity and provenance of certain Microsoft Word documents and emails.
- Acted as an expert witness in a case between two parties who had engaged in a joint venture, producing a report based on the integrity and provenance of certain Microsoft Excel spreadsheets.
- Acted as an expert witness in Imerman v Tchenguiz ([2010] EWCA Civ 908), producing multiple reports based on how certain confidential data had been accessed and used throughout a number of computers and systems.
- Acted as an expert witness in an employment dispute related to activities performed during 'gardening leave'. This involved producing a report detailing the data recovered from a laptop that had been disposed of in a pond and its relevance to the case in hand.
- Acted as an expert witness during a Court of Appeal case producing a report based on the analysis of a number of Word documents.

Forensic Investigations

- Managed multiple forensic investigations in response to Civil Search Orders and Delivery-Up Orders (or similar) whereby data has been securely captured, interrogated and reported on, as instructed by the Court.
- Managed an incident-responsive investigation following the 'hack' of a series of computer systems around the world. This also involved tracing information found during the investigation in order to identify the likely perpetrators.
- Managed a forensic investigation across seven jurisdictions in Europe and the Middle East, identifying relevant data for the lawyers to review related to allegations of corruption prior to an IPO.
- Managed the European aspects of a global forensic investigation relating to a globally coordinated theft of intellectual property.

E-Disclosure

- Managed a multi-jurisdictional e-disclosure project related to a high-profile dispute in the High Court which demanded data was managed in an extremely secure environment both in Russia and the UK.

  Managed an e-disclosure project for a Canadian entity involved in a class-action case in Canada, whereby there was relevant data in the US, Canada, Australia and the UK. This case also involved an expert report dealing with the communication data available compared to what would have been present under the class's allegations.

- Managed an e-disclosure project for a major African bank that was involved in litigation in London but which included the mapping of systems and collection of data in Africa.

Regulatory Response

- Managed all data aspects of an investigation by multiple regulators into the actions of a trader at a global bank. Data from multiple systems and jurisdictions had to be collected, processed and made available for review, including instant-message chat data.
- Managed the disclosure elements of a FCPA investigation being performed by an independent law firm. This involved the on-site capture and processing of data in multiple European countries and the US, as well as dealing with data that was security-classified.
- Managed a large computer forensics raid spread over multiple sites after a series of companies were put into compulsory receivership by the DTI. Subsequent findings and evidence than had to be handed over to the Serious Fraud Office.
- Managed all the data aspects of an investigation by the European Commission into allegations of price-fixing for a global consumer-products company that encompassed data from over 25 countries.

Other

- Acted as an expert adviser to a major African cross-jurisdictional financial authority that had decided to set up, equip, staff and train a forensic computing facility to investigate allegations of internal corruption across the continent.
- Investigated the actions of senior management at a Scandinavian subsidiary of a multi-national energy company, where it had been alleged that suspiciously structured energy trades had been executed.
- Investigated the suspected fraudulent actions of a structured finance trader at a large Japanese bank, where there had been unauthorised deals in a high risk area.

IN THE HIGH COURT OF JUSTICE

BEFORE THE HONOURABLE MR JUSTICE MICHAEL GREEN
DATED 31 July 2023

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
BUSINESS LIST (ChD)

THE AZIMA PROCEEDINGS (Claim no. HC-2016-002798)

B E T W E E N : -

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant / Defendant to Counterclaim

and

FARHAD AZIMA

Defendant / Counterclaimant

and

(1) DAVID NEIL GERRARD
(2) DECHERT LLP
(3) JAMES EDWARD DENNISTON BUCHANAN

Additional Defendants to Counterclaim

KING'S BENCH DIVISION

THE AL SADEQ PROCEEDINGS (Claim no. QB-2020-000322)

B E T W E E N : -

KARAM SALAH AL DIN AWNI AL SADEQ

Claimant

and

(1) DECHERT LLP
(2) NEIL GERRARD
(3) DAVID HUGHES
(4) CAROLINE BLACK

Defendants

THE STOKOE PROCEEDINGS (Claim no. QB-2020-002492)

B E T W E E N : -

STOKOE PARTNERSHIP SOLICITORS

Claimant

and

(5) DECHERT LLP
(6) NEIL GERRARD

Defendants

THE QUZMAR PROCEEDINGS (Claim no. QB-2020-003142)

B E T W E E N : -

JIHAD ABDUL QADER SALEH QUZMAR

Claimant

and

(1) DECHERT LLP
(2) NEIL GERRARD

Defendants

THE GM/KM PROCEEDINGS (Claim no. KB-2023-001231)

B E T W E E N : -

(1) GELA MIKADZE
(2) KHATER MASSAAD

Claimants

and

(1) DECHERT LLP
(2) JAMES BUCHANAN
(3) NICHOLAS DEL ROSSO
(4) VITAL MANAGEMENT SERVICES INC
(a company incorporated in North Carolina)

Defendants

THE BUCHANAN PROCEEDINGS (Claim no. KB-2023-001629)

B E T W E E N : -

JAMES EDWARD DENNISTON BUCHANAN

Claimant

and

STOKOE PARTNERSHIP SOLICITORS

Defendant

B E T W E E N : -

(1) NICHOLAS DEL ROSSO
(2) VITAL MANAGEMENT SERVICES INC

Claimants

and

STOKOE PARTNERSHIP SOLICITORS

Defendant

ORDER

UPON the Claim by Nicholas Del Rosso and Vital Management Services Inc ("**the Del Rosso Parties**"), dated 30 June 2023

AND UPON reading the witness statements of Nicholas Del Rosso, dated 30 June, 14 and 27 July 2023, and the witness statements of Haralambos Tsiattalou of Stokoe Partnership Solicitors ("**Stokoe**"), dated 12 January, 10 May, 20 June and 7 July 2023

AND UPON hearing counsel for the Del Rosso Parties (Adrian Waterman KC, Aidan Wills and Zoe McCallum), for the Stokoe Parties (Gerard Rothschild and Guy Olliff-Cooper), for Dr Massaad and Mr Mikadze (Alastair Tomson), for Mr Azima (Thomas Plewman KC), for Mr Buchanan (Antony White KC), for Mr Findlay (Donald Lilly), for Dechert LLP (Craig Morrison KC) and for Mr Gerrard (Fionn Pilbrow KC and Aarushi Sahore) at the hearing on 31 July 2023

AND UPON the Del Rosso Parties' solicitors, Rosenblatt, undertaking: (i) not to access or examine the Huawei Matebook laptop computer (serial number 2018AP0990: "**the Laptop**") or the Diligence Image (as defined below) prior to the steps set out at paragraph 4 of this Order having been completed; (ii) to retain securely within the jurisdiction the Laptop and a forensic image of the Laptop (produced in accordance with paragraph 4 of this Order) on behalf of the Del Rosso Parties; (iii) that they will not supply the Laptop, the Diligence Image, the forensic image produced pursuant to paragraph 4(b) or (c) of this Order, any Dedicated Media or any Mixed Up Media delivered up pursuant to paragraphs 2(a) and (b) of this Order to the Del

Rosso Parties until the resolution of any disclosure applications pursuant to CPR 31.17 or, in the case of Mr Findlay only, pursuant to CPR 25.1(1)(c)(i) to (iii) and 25.1(1)(i) made within three months of the date of notification to the parties of the Court's approval of the final Order

AND UPON the Del Rosso Parties confirming that they will accept service out of any disclosure applications, made in accordance with the preceding recital, in respect of the Laptop, without requiring the applicants to make an application for permission to serve out, with such applications to be served on Rosenblatt as the Del Rosso Parties' solicitors

AND UPON handing down an *ex tempore* judgment at the hearing on 31 July 2023

IT IS ORDERED THAT:

1. The Del Rosso Parties' claim is allowed.

2. Stokoe shall:
   (a) by 4pm on 11 August 2023, deliver up the Laptop; the image made of the Laptop by Diligence International Limited (the **"Diligence Image"**); and any other dedicated physical media (whether in electronic or hard copy form) containing data derived, extracted, copied or imaged from the Laptop by Stokoe (including by any of its officers, servants or agents) which is in Stokoe's possession, custody or control to Rosenblatt (the "**Dedicated Media**");
   (b) Within 7 days of the date of notification to the parties of the Court's approval of the final Order, deliver up to Rosenblatt a copy of any other data derived, extracted, copied or imaged from the Laptop by Stokoe (including by any of its officers, servants or agents) which is in Stokoe's possession, custody or control (save for data included in materials which have been placed before the Court at public hearings) which is mixed up with other data not in any way so derived, extracted, copied or imaged (the **"Mixed Up Media"**) with redactions so to remove any other data not in any way so derived, extracted, copied or imaged;.
   (c) Within 7 days of the date of notification to the parties of the Court's approval of the final Order, procure the deletion or destruction of any data derived, extracted, copied or imaged from the Laptop by Stokoe contained within the Mixed Up Media, save to the extent that such data has been included in materials which have been placed before the Court at public hearings (except that, for the avoidance of doubt, Stokoe may retain without any deletions one complete copy of the document comprising Diligence's contemporaneous forensic notes); and

(d) Within 7 days of the date of notification to the parties of the Court's approval of the final Order, serve an affidavit confirming that to the best of the deponent's knowledge and belief these steps have been complied with.

3. Within 7 days of the date of notification to the parties of the Court's approval of the final Order, Stokoe will swear and serve an affidavit containing (to the best of their knowledge and belief and save to the extent privileged):

(a) the identity/identities of each person (including any third parties) who has accessed the Laptop since receiving it on 14 July 2022;

(b) the dates on which that access occurred;

(c) the purpose(s) of that access;

(d) full particulars of:

i. the use that Stokoe has made of any data derived, extracted, copied or imaged from the Laptop (save as contained in witness statements, skeleton arguments or in inter partes correspondence with or copied to the Del Rosso Parties in these proceedings or others heard with them), and

ii. the identity/identities of any third parties with/to whom any data derived, extracted, copied or imaged from the Laptop has been disclosed by Stokoe (save as contained in witness statements or skeleton arguments which Stokoe has served on the Del Rosso Parties, or in inter partes correspondence with or copied to the Del Rosso Parties in these proceedings or others heard with them);

(e) a full account of the circumstances in which Stokoe came into possession of the Laptop, and information provided by any third party to Stokoe about the provenance of the Laptop and the data contained thereon;

(f) full particulars of any third parties who Stokoe informed about their receipt and/or possession of the Laptop (save as contained in witness statements or skeleton arguments which Stokoe has served on the Del Rosso Parties, or in *inter partes* correspondence with or copied to the Del Rosso Parties in these proceedings or others heard with them, and save to the extent that information has become public through confirmation by Stokoe at court hearings in relation to the Laptop on 13 January, 2 February 23 June, 21 July and/or 31 July 2023).

Where privilege is relied upon as a basis for not providing information in categories (a)-(f) above, the affidavit shall explain (in relation to each instance of reliance) on what basis privilege is claimed. Where the expression "third parties" is used in this paragraph, it does not include lawyers at Stokoe, or lawyers instructed by Stokoe, Mr Al Sadeq or

Mr Quzmar.

4. Within 7 days of the date of notification to the parties of the Court's approval of the final Order, Rosenblatt shall instruct an independent forensic IT specialist to carry out the following tasks in respect of the Laptop, Diligence Image and Dedicated Media, using reasonable endeavours to complete the tasks within one month of instruction:

   (a) Determine (insofar as is possible) and produce a report ("**the Independent Forensic Report**") addressing the following matters:

      i. whether a backup file of an email account relating to Scott Michael Moore of Moore International PLLC ("**the Moore Data**") is on the Laptop, as alleged by Diligence International Limited in its report of 12 January 2023;

      ii. if so, the date on, and full particulars of how, the Moore Data came to be on the Laptop; and

      iii. details of any access to the Laptop which has taken place since 24 October 2020, including details of when and where that access took place, by whom and what activity and/or operations were performed on the Laptop.

   (b) If the Moore Data is present on the Laptop and/or Dedicated Media:

      i. Remove the Moore Data from the Laptop and Dedicated Media.

      ii. Create a forensic image of the Laptop's hard drive ("**the Amended Laptop Image**").

      iii. Provide the Moore Data to Moore International Law PLLC by a means to be agreed between Rosenblatt and Moore International Law PLLC.

   The preceding steps i-iii are to be conducted prior to returning the Laptop and providing the Amended Laptop Image and Dedicated Media to Rosenblatt.

   (c) If the Moore Data is not present on the Laptop, create a forensic image of the Laptop's hard drive ("**the Laptop Image**").

   (d) Use all reasonable endeavours to search the Laptop for the passcode/password for the Aegis device (including any such password contained within any password manager on the Laptop).

   (e) In performing the above tasks, take steps to minimise the possibility of data on the Laptop or master copies being altered.

5. Rosenblatt shall serve the Independent Forensic Report on Stokoe within 7 days of receiving it.

6. If, pursuant to paragraph 4(d) of this Order, the passcode/password for the Aegis device is located on the Laptop, Rosenblatt shall serve this on the parties to the Azima Proceedings, within 7 days of receiving it, and Rosenblatt shall inform Stokoe of the fact of its having been located.

7. In responding to any applications or orders in respect of documents held on the Laptop Rosenblatt may rely on the Amended Laptop Image or the Laptop Image (as the case may be).

8. Stokoe shall pay the Del Rosso Parties' costs of the claim and their application of 20 February 2023, to be subject to detailed assessment if not agreed.

9. By 4pm on 14 August 2023, Stokoe shall make a payment on account of those costs in the sum of £250,000.

10. This Order shall be served by the Del Rosso Parties on the other parties.

Service of the Order

The Court has provided a sealed copy of this Order to the serving party:

Rosenblatt
165 Fleet Street
London EC4A 2DY
Ref: DEL/23/1

Claimant
H Tsiattalou
16th / 12th / 11th
Exhibit HT16
Dated 12 January 2023

IN THE HIGH COURT OF JUSTICE **Claim No. QB-2020-000322**
KING'S BENCH DIVISION

BETWEEN:

KARAM SALAH AL DIN AWNI AL SADEQ

Claimant

- and -
(1) DECHERT LLP
(2) NEIL GERRARD
(3) DAVID HUGHES
(4) CAROLINE BLACK

Defendants

IN THE HIGH COURT OF JUSTICE **Claim No. QB-2020-002492**
KING'S BENCH DIVISION

BETWEEN:

STOKOE PARTNERSHIP SOLICITORS

Claimant

- and –

(5) DECHERT LLP
(6) MR DAVID NEIL GERRARD

Defendants

IN THE HIGH COURT OF JUSTICE **Claim No. QB-2020-003142**
KING'S BENCH DIVISION

BETWEEN:

JIHAD ABDUL QADER SALEH QUZMAR

Claimant

- and –

(1) DECHERT LLP
(2) NEIL GERRARD

Defendants

Exhibit HT16

This is the exhibit marked "HT16" to the witness statement of Haralambos Tsiattalou dated 12 January 2023.

Instructed By:	Stokoe Partnership Solicitors Second Floor 1 – 3 Staple Inn Holborn London WC1V 7QH
Client Reference:	Reference: AWN001/003/BT

SUMMARY REPORT

of

MICHAEL GEORGE

Diligence Intl Ltd

3rd Floor, 1 Ely Place

Farringdon

London

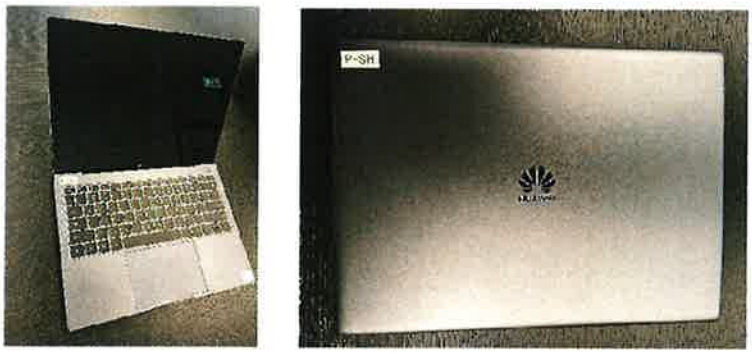
EC1N 6RY

Table of Contents

BACKGROUND

1. This report relates to Stokoe Partnership Solicitors client reference AWN001/003/BT.

2. On the 14th July 2022, Jessica Sarwat of Stokoe Partnership Solicitors delivered to Diligence Intl Ltd the following items:

Description
One (1) Seagate portable drive S/N: NAASFRFT labelled 'USB & JB MBA' 
One (1) x Aegis Padlock 3 A25-3PL256-1000 labelled 'Client' 
One (1) x Huawei Matebook S/N: EHUBB18C10000878 labelled 'P-SH' 

3. The above items were subsequently logged and identified with the following references:

Exhibit Ref.	Description	Sealed As
DFS / 1187	One (1) Seagate portable drive S/N: NAASFRFT labelled 'USB & JB MBA'	E212265
DFS / 1188	One (1) x Aegis Padlock 3 A25-3PL256-1000 Labelled 'Client'	E212266
DFS / 1189	One (1) x Huawei Matebook S/N: EHUBB18C10000878 labelled 'P-SH'	E212267

4. On 28th October 2022, Diligence Intl Ltd received instruction from Stokoe Partnership Solicitors to:

a) Create a forensic working images or images by non-destructive means in accordance with current best forensic practice guidelines.

b) Examine these images to the extent necessary to establish the ownership of the devices.

c) If and to the extent that the ownership of any device is not clear, they should proceed to try to determine the user(s) of the data on the devices.

d) If the objective of identifying the owner(s) of the devices or user(s) of the data cannot be achieved without reviewing the content of any file or data sets, Diligence will produce a list of the content of the devices, halt the process, and revert to Stokoe for further instruction.

EXAMINATION OF DEVICES

DEVICE DFS/1187

5. DFS/1187 is a portable USB drive device detailed as follows:

Device Details: DFS/1187	
Make	Seagate Expansion Portable Drive
Model	SRD0NF1
P/N	1TEAP6-500
S/N	NAASFRFT
Capacity	2TB

6. Using forensic processes and techniques, a forensic image of the above Seagate portable drive was completed using a Logicube Writeprotect Portable write blocker and imaging software FTK Imager v4.3.0.18 resulting in a verified bit-for-bit copy.

7. I produced the following copies of the above Seagate drive DFS/1187.

- Master Copy - DFS1187_MAG_MC1
- Working Copy 1 - DFS1187_MAG_WC1
- Working Copy 2 - DFS1187_MAG_WC2

8. Examination of the physical device did not establish the ownership of this device or the user(s) of the data. The creation of data on the device ranges between October 2009 and August 2020.

9. Examination of file header information identified data on the device which may help to identify potential owner(s) & user(s).

10. In order to identify potential user(s) we looked for the presence of any e-mail accounts or references to email addresses. The following email accounts were identified with a date range of October 2009 to November 2019.

Source Folder: ST-MBA13		eMail Account Reference
Filename:	571715.sqlite	jamie.buchanan@msn.com jamie@rakdev.ae

11. The label on the front of this device contains the wording 'USB & JB MBA' and together with the above identified email addresses, supports that the content of the drive may relate to a person called 'Jamie Buchanan' in some way.

DEVICE DFS/1188

12. DFS/1188 is a portable USB with a built in keypad detailed as follows:

Device Details: DFS/1188	
Make / Model	Apricorn Aegis Padlock 3
Serial No.	P1T036356
Size	1TB
Encryption	256 AES XTS

13. To access this device a six to sixteen-digit PIN code is required to be entered into a keypad located on the front of the drive to access the encrypted data contained therein.

14. According to the 'Apricorn' manufacturer's user manual[1], after up to ten unsuccessful attempts to enter the PIN Code the keypad will lock, after which the drive will assume that it is under brute force attack and automatically delete all of its data.

15. Powering up the device displays a solid red LED which indicates that the drive is locked and is awaiting PIN code entry.

16. Because of the security feature enabled on this device it was not possible to access the data to establish the ownership of this device or the user(s) of the data, no further action was taken on this device.

DEVICE DFS/1189

17. DFS/1189 is a Huawei Matebook laptop containing one (1) solid state drive (SSD) device detailed as follows:

Device Details: DFS/1189	
Make / Model	Huawei Matebook Mach – W29
Serial No.	2018AP0990
SSD Details	
Make / Model	Samsung MZ – VLB5120
P/N	MZVLB512HAJQ-00000
S/N	S3W8NX0KB03735
Manufacture Date	November 2018
Capacity	512GB

18. Using forensic processes and techniques, a forensic image of the above Samsung drive was completed using a Logicube Writeprotect Portable write blocker and imaging software FTK Imager v4.3.0.18 resulting in a verified bit-for-bit copy.

19. I produced the following copies of the above Samsung drive removed from the Huawei Matebook DFS/1189:

[1] https://apricorn.com/content/product_pdf/aegis_padlock/usb_3.0/Aegis_Padlock_3_Manual_sept2022.pdf

- Master Copy – DFS1189_MAG_MC1
- Working Copy 1 – DFS1189_MAG_WC1
- Working Copy 2 – DFS1189_MAG_WC2

20. Initial Examination of the physical device did not establish the ownership of this device or the user(s) of the data. Data on the device ranges between March 2011 and May 2021.

21. 'Windows Registry' files contain user registered details which may assist in determining the device ownership:

Source Files: System32/config/SAM & System32/config/SOFTWARE	
Computer Name	SANTA-HU
Owner	NdR
Operating System	Windows 10
Time Zone	Time Zone: W. Europe Standard Time
Username	NdR
Login Count	83

22. eMail headers contain the above computer name 'Santa-Hu' which is associated with the following eMail address:

- Nick del Rosso - ndr99@email.com

23. Further email addresses were also identified on the device:

- Nick del Rosso - ndr100@usa.com
- Nick del Rosso - ndr@vitalmanage.com
- Leo del Rosso - ndr100@usa.com
- Leo del Rosso (Banking Division) - leo@acceptances.co.uk

24. The username referenced in the Windows registry together with the email header information and other email addresses identified indicate that 'NDR' may relate to a 'Nick Del Rosso'.

25. We also identified a file called 'smm@milopc.com as part of a update24Jan.rar'. This file appears to be a backup file of an email account. A 'Google' search of 'smm@milopc.com' indicates that it relates to a person named Mr Scott Michael Moore within a law firm called 'Moore International Law PLLC' based in New York.

26. The label on the front of this device contains the wording 'P-SH', it is possible that the letters 'SH' may refer to 'Santa HU'.

27. Examination of file header information identified potential owner(s) & user(s) of the device.

CONCLUSIONS

28. Because of the security features enabled on the 'Apricorn Aegis Padlock' USB (DFS1188), it has not been possible to identify the owner or user of the device.

29. It has not been possible to definitively identify the owner of the Seagate portable drive (DFS1187), however the device contains backups or copies of emails relating to 'Jamie.buchanan@msm.com' and 'Jamie@rakdev.ae', and the external label 'USB and JB MBA', suggesting the device is in some way linked to a 'Jamie Buchanan'. The email data represents only part of the total data available.

30. It has not been possible to definitively identify the owner of the Huawei laptop (DFS1189) given it contains multiple e-mail addresses within it, however the data appears to be in some way related to both a 'Scott Michael Moore' and a 'Nick Del Rosso'.

31. Excel spreadsheets of the file headers containing potential user identifiers for both devices (DFS1187 and DFS1189) is available on request, in total they contain over 21,000 file header IDs.

32. We also note that there is similar white labelling adhered to each of the devices which appear to be additional to manufacture labels.

Senior Forensic Investigator – Digital Forensics

Diligence Intl Ltd

Date: 12th January 2023

GENERAL COMMENT

To the best of my knowledge and belief, there are no reasonable grounds for believing that the evidence produced and identified in my report is inaccurate because of improper use of the examining computers.

All computer examinations referred to in this report were carried out in accordance with the 'Association of Chief Police Officers Good Practice Guide for Computer Based Electronic Evidence'.

The accuracy of any timestamps associated with the creation of files, will be dependent on the accuracy of the internal clock of the device that recorded those timestamps. Any dates and times are reported as found.

I reserve the right to amend my opinion should additional data or further information be made available.

I confirm that I have read and understand my duties in relation to the requirements of Part 35 of the Civil Procedure Rules and a signed declaration to that effect is appended to this report.

Although instructions were received from Stokoe Partnership Solicitors, this report is prepared for Court purposes if required.

DISCLOSURE

No methods reported are yet accredited to ISO 17025 but Diligence Intl Ltd work to established and well proven technical procedures and are working towards accreditation. To mitigate any risk of non-accreditation to ISO17025, Diligence Intl Ltd. relies on extensive subject matter experience and operates a quality management system that is accredited to ISO9001:2015 and a security management system that is accredited to ISO27001:2013.

STATEMENT OF TRUTH

I confirm that I have made clear which facts and matters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer.

If any facts subsequently emerge which render any part of this report untrue, I will circulate the fact and all changes to all relevant parties forthwith.

I understand that my primary duty is to the Court when preparing written reports and giving evidence and I have complied and will continue to comply with that duty.

I believe my report to be accurate; it covers the issues raised by my instructions and reflects my views as an independent expert.

Where relevant my report includes any information of which I have knowledge, or of which I have been made aware, that might adversely affect the validity of my conclusions.

I have indicated any sources of information upon which I have relied in my report.

Those instructing me will be informed immediately, with written confirmation, if my existing report requires correction or qualification.

I understand that my report, subject to any corrections before swearing as to its veracity, will form the evidence to be given under oath.

I understand that an expert may assist any cross-examination on my report.

I confirm that I have not entered any arrangement whereby the amount or payment of my fees is in any way dependent on the outcome of the case.

CIVIL DECLARATION

I understand that my overriding duty is to the Court, and I have complied with that duty. I am aware of the requirements of CPR Part 35, its practice direction and the CJC Guidance for the instruction of experts in civil claims.

I confirm that I have made clear which facts and matters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer.

I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

PROFILE

I am a Senior Forensic Investigator at Diligence Intl Ltd and since 1994 I have been directly involved in the investigation and examination of digital data for forensic purposes. I have been trained in data extraction and have considerable experience in using various approved hardware and software tools such as Encase, FTK, XRY, XACT, and a certified Mac Forensic (CMFS) specialist.

I am City & Guilds accredited in CSAS for investigators & analysts, a qualified and approved mobile phone & SIM card examiner, and have been trained in the use of various examination and data extraction equipment and programmes.

I am listed in the UK Register of Expert Witnesses and I have provided expertise and support in a great many criminal and civil cases, for both prosecution and defence, including corporate and commercial investigations

Senior Forensic Investigator – Digital Forensics

Diligence Intl Ltd

Date: 12th January 2023

rosenblatt

165 Fleet Street, London, EC4A 2DY
T +44 (0)20 7955 0880 I F +44 (0)20 7955 0888
www.rosenblatt-law.co.uk

Phil Beckett
Alvarez & Marsal Disputes and Investigations, LLP
Park House
16-18 Finsbury Circus
London
EC2M 7EB

BY EMAIL ONLY: pbeckett@alvarezandmarsal.com
christian.hill@alvarezandmarsal.com

Our Ref: SW/NL/DEL/23/1

16 October 2023

Dear Phil

Claim no. KB-2023-002877 – Nicholas del Rosso & another v Stokoe Partnership Solicitors
Letter of Instruction

1. Thank you for agreeing to act as an independent forensic IT specialist in this matter.

2. As you will see below, this instruction involves: (i) carrying out a forensic examination of the Huawei Matebook laptop computer (serial number 2018A80990) [the "**Laptop**"] belonging to Nicholas Del Rosso ["**Mr Del Rosso**"] and Vital Management Services, Inc ["**VMS**"], which has been delivered up to them by Stokoe Partnership Solicitors ["**Stokoe**"] pursuant to a Court order dated 31 July 2023 (sealed on 9 October 2023) [the "**Order**"]; (ii) removing certain data contained on the Laptop if such data proves to be present and returning it to its owner; (iii) producing a report into the findings of your investigation; and (iv) seeking to locate the password of a separate device, an Aegis Drive.

3. We set out the background to your instruction as follows.

Background

4. The Laptop has been the subject of extremely contentious legal proceedings, which culminated in the Order, pursuant to which Stokoe delivered up the Laptop and the data derived from the Laptop on 11 August 2023.

5. Mr Del Rosso is resident in North Carolina, USA, as is VMS.

6. As at the start of 2020, the Laptop was kept in Mr Del Rosso's London rental flat for use when he was in the UK. As well as personal and business data belonging to him/VMS, the Laptop also contained data belonging to their clients, some of which was subject to privilege and confidentiality considerations.

7. In early 2020, Mr Del Rosso travelled to the USA with the intention of returning to the UK. As such, he left the Laptop in his London flat. However, he was prevented from returning to the UK first by the COVID pandemic and subsequently by very serious health issues that made it impossible for him to travel.

8. As Mr Del Rosso wanted to give up the lease on his London flat, he arranged for the Laptop to be provided to Steve McIntyre ["**Mr McIntyre**"] for safe keeping. Mr McIntyre took possession of the Laptop on 24 October 2020 from Mr Del Rosso's son who was living in London at the time. On 14 July 2022, Mr McIntyre provided the Laptop to Stokoe without Mr Del Rosso's permission, knowledge or consent, in circumstances the Court found were unlawful. Stokoe was thus ordered to deliver up the Laptop to Mr Del Rosso and VMS.

9. It is not necessary to go into detail of the Delivery Up claim, save for the following.

10. Stokoe's resistance to Mr Del Rosso and VMS's claim arose in great part from a report into the Laptop dated 12 January 2023 prepared by Diligence International Limited ["**Diligence**"] [the "**Diligence Report**"]. This report contained reference to the existence of data on the Laptop belonging to a third party, Scott Michael Moore ["**Mr Moore**"] of Moore International PLLC ["**Moore International**"], a US law firm [the "**Moore Data**"]. The provenance of the presence of the Moore Data was an issue of great significance, as Stokoe alleged that Mr Del Rosso and VMS were involved in the hacking of data and that the existence of the Moore Data on the Laptop was evidence of this.

11. Stokoe therefore heavily relied on the reported presence of the Moore Data on the Laptop as a reason not to deliver it up. However, Mr Del Rosso and VMS were never instructed to carry out work in respect of Mr Moore or Moore International, and, assuming that it is on there, the Moore Data must have been put on the Laptop by someone other than Mr Del Rosso. The Laptop was therefore delivered up to Mr Del Rosso/VMS in part on the basis that an investigation would be carried out as to how and when the Moore Data came to be on the Laptop, assuming that it is on there.

12. A number of parties in other legal proceedings have expressed a desire to seek disclosure from the Laptop, again on the basis that Mr Del Rosso and VMS are alleged to have been involved in hacking and they suspect that such material may be on there. As such, it was also agreed as part of the delivery up process that the Laptop would be provided to us as Mr Del Rosso's/VMS's English solicitors to ensure that it remained in the jurisdiction for the time being.

13. Moreover, in order to protect the confidentiality of the Moore Data, it was agreed that, before Rosenblatt were to view the Laptop, the Moore Data would be removed from the Laptop and also from any other dedicated physical media, including an image of the Laptop made by Diligence, known as the "**Diligence Image**". All of this other physical media, including the Diligence Image, is described in the Order of the Court as the "**Dedicated Media**".

14. A question that has arisen following the hearing that took place on 31 July 2023 at which Delivery Up of the Laptop and its associated media was ordered is that Stokoe have stated that they only learnt since then that the date settings on the Laptop are claimed to be approximately one year out. Please see paragraph 20 of the Affidavit of Haralambos Tsiattalou dated 11 September 2023 for further details.

15. In addition to the Laptop, Mr Del Rosso provided Mr McIntyre another device for safe keeping: an Aegis Drive. Although purchased by Mr Del Rosso/VMS, this device contained data belonging to Dechert LLP, over which Mr Del Rosso and VMS have sought to exercise no rights. The Aegis Drive is the kind that, after a certain amount of incorrect password entries, it will automatically wipe all of its content. Mr Del Rosso has been unable to recall the password to the Aegis Drive. Stokoe and their associated parties seek disclosure from this device also, and believe the password to the Aegis Drive may be located on the Laptop.

Enclosures with these Instructions

16. To assist you in this instruction, we enclose the following documents:

    a. The Order, which sets out the process for you to follow at paragraph 4.

    b. The Diligence Report.

    c. Key Evidence from the Delivery Up claim relating to the Moore Data, including:

        i. The Statements of Mr Del Rosso dated 30 June 2023 (and Exhibit) and 14 July 2023;

        ii. The Statements of Haralambos Tsiattalou, partner at Stokoe, dated 12 January 2023, 10 May 2023, 20 June 2023 and 7 July 2023.

        iii. Transcript from the hearing on 31 July 2023.

        iv. Approved judgment relating to delivery up.

        v. The Affidavit of Haralambos Tsiattalou dated 11 September 2023.

        vi. A folder of photographs showing the various items as delivered up.

    d. If you need any further documents, please let us know and we will provide them to you as soon as possible.

The Laptop and Associated/Dedicated Media

17. The Laptop and its associated media including the Dedicated Media are securely stored in our offices. Each item is contained within a sealed, numbered bag, which are then contained in one large, sealed

and numbered bag. The Laptop and associated media and the Dedicated Media were provided to us in this fashion by Stokoe and were promptly placed in a secure storage device after receipt. Since this time, we have not sought to access the Laptop or any of the other material provided to us by Stokoe.

18. Once you have reviewed these instructions, please inform us as to how best to provide you with the Laptop and associated media and the Dedicated Media so as to ensure they are received by you in the manner by which they were provided to us by Stokoe, so as to avoid there being any suggestion that the Laptop, associated media or Dedicated Media have been accessed in any way by us (or anyone else) in the meantime.

Instructions

19. Upon collection of the Laptop and the associated/Dedicated Media, please will you:

    a. Record the condition upon which you have taken receipt of all items.
    b. Review all items provided so as to verify that they accord with the signed Summary of Media provided by Stokoe on 11 August 2023.
    c. Review all items so as to be able to carry out the requirements of the investigations pursuant to the Order as follows.

20. As set out in the Order at paragraph 4:

    a. Determine (insofar as is possible) and produce a report ["**the Independent Forensic Report**"] addressing the following matters:

        i. whether a backup file of an email account relating to Scott Michael Moore of Moore International PLLC ["**the Moore Data**"] is on the Laptop, as alleged by Diligence International Limited in its report of 12 January 2023 (Paragraph 4(a)(i));
        ii. if so, the date on, and full particulars of how, the Moore Data came to be on the Laptop (Paragraph 4(a)(ii)); and
        iii. details of any access to the Laptop which has taken place since 24 October 2020, including details of when and where that access took place, by whom and what activity and/or operations were performed on the Laptop (Paragraph 4(a)(iii)).

    b. If the Moore Data is present on the Laptop and/or Dedicated Media:

        i. Remove the Moore Data from the Laptop and Dedicated Media (Paragraph 4(b)(i)).
        ii. Create a forensic image of the Laptop's hard drive ["**the Amended Laptop Image**"] (Paragraph 4(b)(ii)).
        iii. Provide the Moore Data to Moore International Law PLLC by a means to be agreed between Rosenblatt and Moore International Law PLLC (Paragraph 4(b)(iii)).
        iv. The preceding steps i-iii are to be conducted prior to returning the Laptop and providing the Amended Laptop Image and Dedicated Media to Rosenblatt.

c. If the Moore Data is not present on the Laptop, create a forensic image of the Laptop's hard drive ["**the Laptop Image**"] (Paragraph 4(c)).

d. Use all reasonable endeavours to search the Laptop for the passcode/password for the Aegis device (including any such password contained within any password manager on the Laptop) (Paragraph 4(d)).

e. In performing the above tasks, take steps to minimise the possibility of data on the Laptop or master copies being altered (Paragraph 4(e)).

f. Prepare a report that sets out your findings pursuant to 20(a) above (Paragraph 4(a)). In your report, please address the issue as to whether or not the date settings on the Laptop are approximately one year out.

g. Provide the Aegis Drive password, if located, and set out the search terms utilised when looking for the password, to us (Paragraph 6).

21. Paragraph 4 of the Delivery Up Order requires that you use reasonable endeavours to complete the tasks within one month of your instruction, i.e. by 16 November 2023. If at any point you consider further time will be necessary, please let us know.

22. Once you have reviewed these instructions, we would like to meet with you to discuss the parameters of your report. We will be happy to provide you with supplemental instructions at any stage should you require, including upon having carried out your initial review of the Laptop and associated and Dedicated Media.

23. In carrying out your instructions, please ensure that you keep a detailed record of all actions taken in respect of each item.

24. When you have completed your work, please return all of the items to us. In respect of the Diligence Image, please will you provide this to us in a sealed, numbered bag.

25. We hope above is clear, but we are of course happy to discuss any matter and provide any further information you need as required.

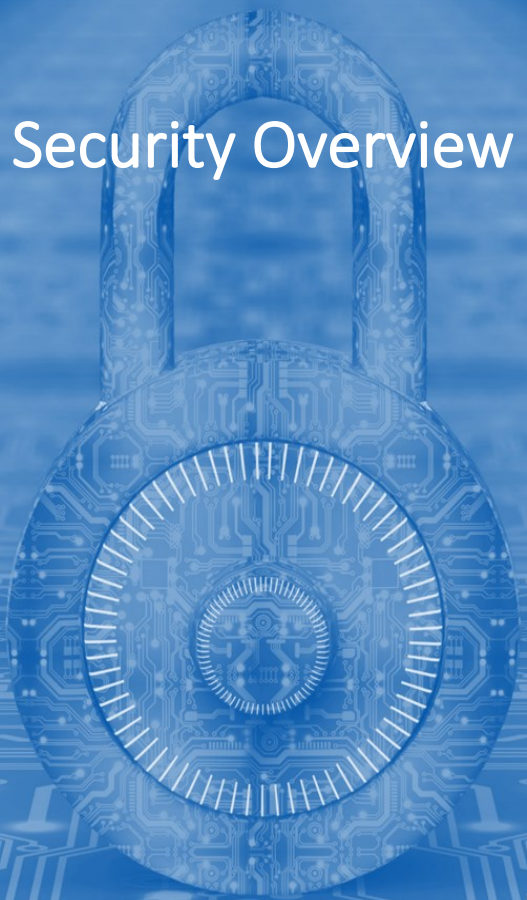
Yours faithfully

Rosenblatt

ROSENBLATT
Encs.

EMEA FORENSIC TECHNOLOGY SERVICES

Security Overview



Overview

At Alvarez & Marsal (A&M), we understand our role as trusted stewards for our clients' most important and valuable assets: their data. A&M's Cybersecurity Program employs a layered, defense-in-depth strategy to protect information assets and systems. Core pillars of this Program include Data Governance, Boundary Defense, Access Control, Endpoint Security, Threat Prevention/Monitoring, Vulnerability Management, Business Continuity, Physical Security, and enterprise-wide Security Awareness. These safeguards and a dedicated security function have been implemented to ensure the confidentiality, integrity, and availability of A&M and client data.

A&M Disputes & Investigations maintain ISO/IEC 27001:2017 certification for our datacentres and forensic labs in the UK under Certificate Registration No. 12 310 62597 TMS, in Germany under Certification No. 12 310 56289 TMS and in Switzerland under Certification No. 12 310 63257 TMS issued by The Certification Body of TÜV SÜD Management Service GmbH. Each site is audited annually. Additionally, in line with the firm's commitment to cybersecurity, A&M is Cyber Essentials certified, which consists of an annual independent third-party assessment of A&M's security practices.

The ISO 27001 framework informs and supports all security related objectives, policies, and procedures including:

- Access control and management
- Security event and access monitoring
- Information system monitoring
- Network intrusion detection
- Network perimeter firewalls
- Multi-factor authentication
- Physical and environmental protection
- Contingency planning
- Backup and recovery
- Media handling and protection
- Vulnerability assessment
- Patch management
- Personnel screening
- Configuration management
- Change management
- Transmission encryption
- Malicious code protection
- Audit review, analysis, and reporting
- Security awareness and training
- Controlled system maintenance

Boundary Defence

Respective of perimeter protection, next-generation Firewalls and Intrusion Detection/Prevention Systems are utilized along the network edge to filter/block malicious and non-standard traffic. Access to Internet domains is further filtered based upon threat indices (e.g., known bad) and reputational factors. Emails entering A&M's network are scanned using multiple layers of technologies for malware, and to proactively detect and block phishing attempts. Further validation of A&M's external posture is determined through a combination of internal and external vulnerability scanning, external penetration testing, and using an independent third-party security scorecard/ratings platform which continuously scans the network edge for security indicators including but not limited to botnet infections, spam propagation, malware, open ports, and TLS/SSL certificates/ misconfigurations.

Endpoint Protection

Careful consideration has been placed on securing the endpoint and thus protecting the information of our clients. Firm laptops are firstly configured with whole disk encryption (encryption at rest) along with pre-boot PIN, ensuring all content on the disk is encrypted utilizing industry standard AES symmetric encryption. Laptops are further hardened to include A&M's security stack, inclusive of local firewall configuration, anti-virus (with automatic updates), next-generation malware protection (advanced sandboxing, continuous analysis, malware blocking), and DNS layer content filtering functional on and off the corporate network. Security patches are applied in a consistent, prompt manner reviewed by A&M's Security Operations team to determine risk and applicability. Data residing on the endpoint is backed-up centrally several times per day, preventing data loss respective of availability.

Secure Data Transmission & Storage

A&M recognizes the importance of supplying a secure collaborative workspace for information. When agreed upon with the client, A&M can provide the use of Citrix ShareFile with storage zones in each of our EMEA data centres to facilitate secure collaboration and data sharing while enforcing both encryption at rest (AES) and in transit (TLS). Client data is logically separated, with access strictly controlled at the file/folder level backed by detailed audit logs. Multi-factor Authentication and Information Rights Management (file-level encryption, monitoring, tracking, and near real-time access revocation) capabilities are also used.

Security Monitoring & Incident Response

Core to A&M's Security Program is the continuous monitoring of security data to identify and quickly respond to potential cyber threats. A&M uses industry-leading tools to identify security vulnerabilities followed by analysis and timely remediation. Dark web threat intelligence provides A&M early warning signals to prevent account compromise. Log data from A&M's security stack is centrally collected and managed within a Security Information and Event Management (SIEM) platform. This platform along with others, is monitored 24/7 by A&M's Security Operations Center (SOC) function; a global team comprised of seasoned Security professionals. A&M's Security Incident Response Plan establishes the framework governing the response lifecycle through Identification, Containment, Eradication & Recovery.

Security Awareness

Supported by firm leadership, Security Awareness Training (covering cyber hygiene) is provided to all employees as part of the on-boarding process and biennially afterwards. Periodic messaging and training content is delivered to all workforce members based upon the current cyber threat landscape. Additionally, the forensic technology team must undergo annual ISO 27001 training. When working with especially sensitive and/or regulated data, additional security training may be provided.

Physical Security

Physical security is supported using badge access readers within A&M corporate offices, whereby compartmentalized areas are restricted to authorized personnel. A combination of CCTV/cameras, visitor logs, and capabilities coordinated with building management are utilized. At the user-level, employees are provided with privacy screens to ensure data is protected from public view.

Data Centre and Forensic Lab Security

A&M Forensic Technology Services co-located data centres and forensic labs are designed to provide the highest levels of security and availability—strict enough to meet and exceed the stringent requirements of our most heavily-regulated financial institution clients. Physical access is controlled and monitored by professionals within A&M's FTS practice and operations staff on-premises 24/7/365, biometric access controls, access logging and security cameras.

A&M FTS has three geographically dispersed co-located data centers in EMEA. These data center partners have obtained control reporting standard certifications and have undergone independent security audits from leading financial services and technology companies. These certifications, renewed annually, guarantee that the highest levels of security, availability, integrity, and confidentiality controls are continuously maintained within each of A&M's hosted data center environments.

Co-location Partner	Certifications
Interxion (London, UK)	ISO/IEC 27001, ISO 22301, SOC-2 Type II, PCI DSS
Noris Network AG (Munich, DE)	ISO/IEC 27001, ISO 90001, SOC-2 Type II, PCI-DSS
Interxion AG (Opfikon, CH)	ISO/IEC 27001, ISO 22301, SOC-2 Type II, PCI DSS

Each of A&M's dedicated co-located data centers uses an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. All areas of A&M's data centers are monitored and recorded using CCTV, and all access points are controlled. Each data center is staffed with 24-hour security officers; visitors are screened upon entry to verify identity and are escorted to authorized locations based on access permissions controlled exclusively by A&M personnel. Full access history is recorded and is available for audit by A&M and its clients.

A&M's co-located data centers includes the following security and environmental features:

- 24x7x365 security staff
- Data centre areas have windowless exteriors
- Biometric readers
- Kinetic and key locks on closed cabinets
- CCTV digital camera coverage of the entire center, including cages, with detailed surveillance and audit logs
- N+1 redundant power
- Uninterruptible Power Supply to prevent power spikes, surges, and brownouts
- Redundant backup diesel generators
- Temperature and humidity control
- Fire detection and suppression
- Visitor access controls

Business Continuity

Client data residing on A&M servers are safeguarded from data-loss through automated back-up and replication to a secondary data centre. All collocated data centers are designed to withstand severe weather and other regional risks and are purpose built for redundancy with established failover procedures. A&M has established a Business Continuity framework to support business resiliency, consisting for four major pillars:

- Business Impact Analysis – Understand the impact to business operations during a disaster scenario in which the facility in either inaccessible or impaired for an extended period. This analysis will identify dependencies on the facility, single points of failure, and technologies utilized.
- Facility Risk Assessment – Identify risks relative to the facility; understand the effectiveness of existing controls and perform pre-planning to mitigate risk.
- Business Continuity Plan – Establishes the framework and procedures to "Keep the Business in business until business operations return to normal."
- IT Disaster Recovery Plans – IT procedures to recover data and systems within right timeframes.

Confidentiality

Applying the concept of least privilege, A&M takes a variety of steps to limit access to client data to only those individuals authorized to access this data by virtue of their delivery role. A&M's standard client engagement letter includes formal provisions addressing confidentiality requirements for all data and information received by our clients. For most engagements, client-specific electronic data rooms and project folders are established and maintained throughout the project's life, limiting access to authorized individuals with necessary and defined roles in support of the engagement. These individuals are instructed in advance of their involvement regarding all engagement-specific confidentiality requirements.


A
&
M

Chronology of Forensic Artefacts

Exhibit PB2-01

#	Date	Forensic Artefact	Application	Type	Activity / Event Description
1	14/10/2019 10:15:47	Jump Lists	Windows Explorer/Microsoft Word	Password File Created on F: Volume	"F:\ADMIN\ADMIN\PASSWORDS.docx" Date Created on Apricorn Aegis Fortress L3 USB Device
2	14/10/2019 10:15:47	Microsoft Office Backstage Items	Microsoft Word	Recovery Keys Folder on F: Volume	"F:\ADMIN\ADMIN\RECOVERY KEYS" Last Modified Date on Apricorn Aegis Fortress L3 USB Device
3	11/11/2019 13:14:44	USB Artefacts (Windows Registry)	USB Device Connected	Apricorn Aegis Fortress L3 USB Device is Connected	Apricorn Aegis Fortress L3 USB Device is Connected
4	10/01/2020 20:16:52	Jump Lists	Windows Explorer/Microsoft Word	Password File Last Accessed/Modified on F: Volume	"F:\ADMIN\ADMIN\PASSWORDS.docx" Last Accessed/Modified on Apricorn Aegis Fortress L3 USB Device

Redacted

18	31/01/2020 10:48:03	User Assist Windows Registry	CCleaner	CCleaner	CCleaner last run date
19	31/01/2020 10:48:57	Windows Timeline	Microsoft Word	Accessing Password File	Microsoft Word application **Start Time.** File "F:\ADMIN\ADMIN\PASSWORDS.docx" is open within the application. (The application was open/in focus)
20	31/01/2020 10:50:50	Jump Lists/LNK Files	Windows Quick Access	Password File Last Modified Date	"F:\ADMIN\ADMIN\PASSWORDS.docx" Last Accessed/Modified Date
21	31/01/2020 10:50:54	Windows Timeline	Microsoft Word	Application End Time	Microsoft Word application **End Time**
22	31/01/2020 10:51:38	USB Artefacts (Windows Registry) and Windows Event Logs	USB Device Removed	Apricorn Aegis Fortress L3 USB Device is removed (F:)	Apricorn Aegis Fortress L3 USB Device is removed (F:)
23	31/01/2020 10:55:16	Folders/Files	CCleaner	CCleaner File Created Date	CCleaner drive wiping Z file Date Created
24	31/01/2020 10:59:00	Folders/Files	CCleaner	CCleaner File Last Accessed/Modified Data	CCleaner drive wiping Z file Last accessed/Modified date
25	31/01/2020 10:59:01	Folders/Files	CCleaner	CCleaner File Created Date	CCleaner drive wiping Z file Date Created
26	31/01/2020 11:02:03	Folders/Files	CCleaner	CCleaner File Last Accessed/Modified Data	CCleaner drive wiping Z file Last accessed/Modified date

Redacted